U.S. Department of Energy
Office of River Protection
Mr. Michael K. Barrett
Contracting Officer
P.O. Box 450, MSIN H6-60
Richland, Washington 99352

CCN: 038768

Dear Mr. Barrett:

CONTRACT NO. DE-AC27-01RV14136 – TRANSMITTAL FOR APPROVAL – AUTHORIZATION BASIS CHANGE NOTICE 24590-WTP-ABCN-ESH-01-029, REVISION 1, *ADDITION OF RISK REDUCTION CLASS (RRC) ITEMS TO SRD*

References: 1) CCN 033734, Letter, R. C. Barr, ORP, to R. F. Naventi, BNI, "Office of Safety Regulation Review of Standards Approval Package and Associated Authorization Basis Change Notices in Support of the "SRD Standards Approval Package Submittal" ABCN 24590-WTP-ESH-01-029," 02-OSR-0204, dated May 14, 2002.

2) CCN 027626, Letter,A. R. Veirup, BNI, to M. K. Barrett, ORP, "Transmittal for Approval: Contract Deliverable "Revised Standards Approval Package – Update" and Associated Authorization Basis Change Notices in Support of the "SRD Standards Approval Package Submittal,"dated February 5, 2002.

Bechtel National, Inc. (BNI) is submitting Authorization Basis Change Notice (ABCN), 24590-WTP-ABCN-ESH-01-029, Revision 1, to the U.S. Department of Energy (DOE), Office of River Protection and the Office of Safety Regulation (OSR) for approval (attached). This ABCN proposes the concept of Risk Reduction Class as a subset of Important-To-Safety (ITS) items, as defined in DOE/RL-96-0006, into the WTP project design.

Approval of this ABCN is requested by October 15, 2002 to support Low Activity Waste/High Level Waste Construction Authorization.

An electronic copy of ABCN 24590-WTP-ABCN-ESH-01-029, Revision 1, is provided for the OSR's information and use.

Please contact Mr. Bill Spezialetti at (509) 371-4654 for any questions or comments.

Very truly yours,

A. R. Veirup
Prime Contract Manager

TR/slr

Attachment: Authorization Basis Change Notice (ABCN), 24590-WTP-ABCN-ESH-01-029, Revision 1, plus attachments

cc: Name (ALPHABETIZE)	Organization	MSIN
Barr, R. C. w/a (1 hard copy and 1 electronic copy)	OSR	H6-60
Beranek, F. w/o	WTP	MS6-P1
Betts, J. P. w/o	WTP	MS4-A1
Dickey, R. L. w/a	WTP	MS6-R1
DOE Correspondence Control w/a	ORP	H6-60
Erickson, L. w/a	ORP	H6-60
Garrett, R. L. w/o	WTP	MS6-P1
Gibson, K. D. w/a	WTP	MS6-R1
Klein, D. A. w/a	WTP	MS6-P1
Naventi, R. F. w/o	WTP	MS4-A1
Nakao, R. M. w/a	WTP	MS4-B2
Ollero, J. E. w/o	ORP	H6-60
PDC w/a	WTP	MS5-K1
QA Project Files w/a	WTP	MS4-A2
Ryan, T. B. w/a	WTP	MS6-R1
Spezialetti, W. R. w/o	WTP	MS6-P1
Struthers, D. J. w/o	ORP	H6-60
Swailes, J. H. w/a	ORP	H6-60
Taylor, W. J. w/a	ORP	H6-60
Veirup, A. R. w/o	WTP	MS4-A1

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-029 Revision 1

ABCN Title Addition of Risk Reduction Class (RRC) Items to SRD

I. ABCN Review and Approval Signatures

A. ABCN Preparation

Preparer:	T. R. McDonnell		
	Print/Type Name	*Signature*	*Date*
Reviewer:	J. Hinckley		
	Print/Type Name	*Signature*	*Date*

B. Required Reviewers

Review Required? *For each person checked, that signature block must be completed.*

Review Required?	Reviewer	Print/Type Name	Signature	Date
☒	ES&H Manager	Fred Beranek		
☒	QA Manager	George Shell		
☒	PSC Chair	Bill Poulson		
☐	Commissioning/Training Manager			
☒	Engineering Manager	Fred Marsh		
☐	Construction Manager			
☐	Area Project Manager			
☐	Research & Technology Manager			
☒	PMT Chair	Richard Garrett		
☐	Other Affected Organization			
☐	Other Affected Organization			
☐	Other Affected Organization			

C. ABCN Approval

WTP Project Manager	Ron Naventi		
	Print/Type Name	*Signature*	*Date*

ABCN Number 24590-WTP-ABCN-ESH-01-029 Revision 1

ABCN Title Addition of Risk Reduction Class (RRC) Items to SRD

II. Description of the Proposed Change to the Authorization Basis

D. Affected AB Documents:

Title	Document Number	Revision
Safety Requirements Document Volume II	24590-WTP-SRD-ESH-01-001-02	1c

Decision to Deviate ☐ Yes ☒ No

If yes, DTD Number/Revision ____________ DTD Closure Date: ____________

Initiating Document Number/Revision Contract No. DE-AC27-01RV14136

E. Describe the proposed changes to the Authorization Basis Documents:

Rewrite SRD Volume II, Safety Criteria 1.0-8, 4.1-3, 4.1-4, 4.2-4, 4.3-1, 4.3-3, 4.3-4, 4.4-2, 4.4-4, 6.0-4, 7.0-2, 7.4-1, Appendix A and Appendix B per Attachment 1, Safety Requirements Document (SRD), 24590-WTP-SRD-ESH-01-001-02, Proposed Changes. These changes are on pages 1-3 and 1-4 (Rev. 1); 4.1-3 and 4.1-6 (Rev. 1c); 4.2-2, 4.3-1, and 4.3-2 (Rev. 1); 4.4-1 (Rev. 1a); 6-2 (Rev. 1); 7.0-1 (Rev. 1); 7.4-1 (Rev. 1c), A-16 (Rev. 1); B-3, B-16, B-17, B-19, B-20, B-21, and B-22, (all Rev. 1).

For SRD Volume II, Safety Criteria 4.3-1, 4.3-3, 4.3-4, 4.4-2 and 4.4-4 clarify which implementing standards apply to SDC, SDS and RRC. Added SRD Volume II, Appendix A, Implementing Standard for Safety Standards and Requirements Identification as an implementing standard for Safety Criteria 4.2-4, 4.3-1, 4.3-3, 4.3-4, and 4.4-2. These changes are on pages 4.2-2, 4.3-1, 4.3-2 (Rev. 1); and 4.4-1 (Rev. 1a).

Update SRD Volume II, Appendix B, Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth, sections 6.2, 6.3, 6.4, 6.5, and 6.8 per Attachment 1. These changes are on pages B-19 through B-21 (Rev. 1).

Update SRD Volume II, Appendix C, Implementing Standards, Section 4.0, per Attachment 1. This change is on page C.4-1 (Rev. 1).

Update ISMP Section 1.3.10, Classification of Structures, Systems, and Components to include new Important to Safety category – Risk Reduction Class (RRC). These changes are on pages 1-16 and 1-19, both revision 0.

Revise section 3.3.8 of the General Information of the PSAR to Support Partial Construction Authorization to include new Important to Safety category – Risk Reduction Class (RRC). This change is on page 3-14, revision 0.

F. List associated ABCNs and AB documents, if any:

- 24590-WTP-ABCN-ESH-01-001, *Revision to ISM Process & Defense in Depth (Appendices A & B)*
- 24590-WTP-ABCN-ESH-01-002, *Selection of Implementing Standard for Startup*

G. Explain why the change is needed:

Change is needed to fully implement the concept of Important to Safety, as defined in DOE/RL-96-0006 into the WTP project design.

H. List the implementation activities and the projected completion dates:

Activity	**Date**
Inform DOE that AB has been revised and formally transmit electronic version	30 days or less after DOE

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-029 Revision 1

ABCN Title Addition of Risk Reduction Class (RRC) Items to SRD

H. List the implementation activities and the projected completion dates:

Activity	**Date**
	approval
Distribute revised controlled copy pages / update WTP Library	30 days after DOE approval

Revise the following implementing documents:

Documents		**Describe extent of revisions**	**Date**
1	GPP-SANA-002	Editorial changes to incorporate RRC	30 days after DOE approval
2	GPP-SANA-003	Editorial changes to incorporate RRC	30 days after DOE approval
3	GPG-SANA-002	Editorial changes to incorporate RRC	30 days after DOE approval
4	GPG-SANA-001	Editorial changes to incorporate RRC	30 days after DOE approval

Describe other activities:		**Date**
1	Revise Safety Analysis Reports, SIPD to incorporate RRC	30 days after DOE approval
2		

III. Evaluation of the Proposed Change

I. Is DOE approval required? Answer questions for Administrative Control changes OR Facility changes, not both.

For an Administrative Control change: **Yes** **No**

1. Does the revision involve the deletion or modification of a standard previously identified or established in the SRD? ☐ ☐

   Explain:

2. Does the revision result in a reduction in commitment currently described in the AB? ☐ ☐

   Explain:

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-029 Revision 1

ABCN Title Addition of Risk Reduction Class (RRC) Items to SRD

3. Does the revision result in a reduction in the effectiveness of any procedure, program, or plan described in the AB? ☐ ☐

   Explain:

For a Facility (technical) change: **Yes** **No**

1. Does the revision involve the deletion or modification of a standard previously identified or established in the SRD? ☒ ☐

   Explain:

   This revision expands the scope of Important to Safety to include Risk Reduction Class (RRC) – items not designated as SDC or SDS. For affected SRD Safety Criteria (see section II.e), this revision specifically defines which implementing standards apply to SDC, SDS, and RRC items.

2. Does the revision create a new Design Basis Event (DBE)? ☐ ☒

   Explain:

   This revision deals with safety classification of SSCs; no facility modification that could lead to creation of a new DBE has been made.

3. Does the revision result in the more than a minimal increase in the frequency or consequence of an analyzed DBE as described in the Safety Analysis Report? ☐ ☒

   Explain:

   This revision deals with safety classification of SSCs; no facility modification that could lead to an increase in frequency or consequences of a DBE has been made.

4. Does the revision result in more than a minimal decrease in the Safety Functions of important-to-safety SSCs or change how a Safety Design Class SSC meets its respective safety function? ☐ ☒

   Explain:

   This revision deals with safety classification of SSCs; no facility modification that could lead to a decrease in the Safety Function of an ITS SSC has been made.

J. Complete the safety evaluation by describing how the revision to the AB:

1. will continue to comply with all applicable laws and regulations (e.g., 10 CFR 830, 10 CFR 835), conform to top-level safety standards (e.g., DOE/RL-96-0006), and provide adequate safety.

   The WTP safety classification approach implemented by this revision is broader than that in 10 CFR 830. Attachment 6 to this ABCN provides a detailed discussion of conformance with the top-level safety standards and provision of adequate safety.

2. will continue to conform to the contract requirements associated with the authorization basis document(s) affected by the revision.

   Attachment 5 to this ABCN provides a detailed discussion of conformance with the contract requirements associated with the authorization basis document(s).

Authorization Basis Change Notice

ABCN Number 24590-WTP-ABCN-ESH-01-029 Revision 1

ABCN Title Addition of Risk Reduction Class (RRC) Items to SRD

3. will not result in inconsistencies with other commitments and descriptions contained in portions of the authorization basis or an authorization agreement not being revised.

   Attachment 5 to this ABCN demonstrates that this proposed change will not result in inconsistencies with other commitments and descriptions contained in portions of the authorization basis or an authorization agreement not being revise.

K. Justification of the Proposed Change

If the change requires DOE approval, provide a justification that demonstrates that the proposed change is safe.

Attachment 5 to this ABCN demonstrates that this proposed change is safe.

L. Certification of Continued SRD Adequacy

Based on evaluations from III.I, if either question III.I.1 is marked "Yes", Project Manager certification is required. The Project Manager's signature certifies that the revised SRD continues to identify a set of standards that provides adequate safety, complies with WTP applicable laws and regulations, and conforms with top-level safety standards and principles. This certification is based on adherence to the DOE/RL-96-0004 standards identification process and successful completion of review and confirmation by the PSC.

WTP Project Manager:	Ron Naventi		
	Print/Type Name	*Signature*	*Date*

M. List of Attachments

1. Safety Requirements Document (SRD), 24590-WTP-SRD-ESH-01-001-02, Proposed Changes
2. Integrated Safety Management Plan (ISMP), 24590-WTP-ISMP-ESH-01-001, Proposed Changes
3. SRD Proposed Changes Summary Evaluation
4. Preliminary Safety Analysis Report to Support Partial Construction Authorization; General Information, 24590-WTP-ABCN-ESH-01-029, Proposed Changes
5. Summary of ISM Process for Revision to Implementing Standards and Safety Criteria
6. Safety and Conformance Evaluation

Safety Criterion: 1.0 - 7

To compensate for potential human and equipment failures, a defense-in-depth strategy shall be applied to the facility commensurate with the hazards; such that, as appropriate to control the risk, safety is vested in multiple, independent safety provisions, no one of which is to be relied upon excessively to protect the public, the workers, or the environment. This strategy shall be applied to the design and operation of the facility.

Implementing Codes and Standards

ANSI/ANS 58.9-1981 Single Failure Criteria for Light Waster Reactor Safety-Related Fluid Systems
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety 4.1.1.2
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

Regulatory Basis

DOE/RL-96-0006 *4.1.1.1 Defense in Depth-Defense in Depth*

Safety Criterion: 1.0 - 8

Structures, systems, and components (SSCs) that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public are classified as Important to Safety. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation). This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of Important to Safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

Important to Safety includes SSCs designated as Safety Design Class, ~~and~~ Safety Design Significant, and Risk Reduction Class.

Safety Design Class (SDC). Safety Design Class SSCs are the following:

1) SSCs~~s~~ ~~that~~whose safety function is to prevent a worker or the maximally exposed member of the public from receiving a radiological exposure that exceeds the exposure standards defined in the SRD;

2) SSCs whose safety function is to ~~that~~ prevent a worker or the maximally exposed member of the public from receiving a chemical exposure that exceeds the exposure standards defined in the SRD; or
3) SSCs ~~that are~~ credited for the prevention of a criticality event.

Safety Design Significant (SDS). Safety Design Significant SSCs are the following:

1) SSCs that are required to ensure that exposure standards for normal operation are not exceeded;
2) SSCs whose failure would directly prevent Safety Design Class SSCs from performing their safety function ~~(e.g., Seismic II/I items)~~; ~~; or~~
2) ~~SSCs that are required to meet the target frequency or barrier requirements of the SRD Appendix B, *Implementing Standard for Defense in Depth,* Section 3.0, Table 1, *Implementation of Defense in Depth by SSCs.*~~ or
3) SSCs that are required to meet SRD Appendix B, section 3.0, Table 1, "Implementation of Defense in Depth by SSCs."

Risk Reduction Class (RRC). RRC SSCs are ~~the following:~~

~~SSCs that are provided to ensure a return to normal operation or to bring the facility to a safe condition in the event of anticipated, but abnormal events that involve radioactive material. These SSCs may provide automatic system response to such events or may be SSCs such as monitors or alarms that alert operators to the necessity of taking manual action;~~
~~SSCs not designated as SDC or SDS that comprise the primary barrier against radioactive material (SL-1, SL-2, and SL-3 events) or chemical (Above Threshold) releases;~~
~~SSCs not designated as SDC or SDS that comprise the secondary barrier against radioactive material or chemical releases, where the primary barrier is SDC or SDS, or;~~
~~SSCs that are identified as significant contributors to safety by the analyses that confirm the facility accident risk goals are met.~~Important to Safety SSCs that are neither SDC nor SDS.

~~Safety Design Class SSCs includes those that, by performing their specified safety function, prevent workers or the maximally exposed member of the public from receiving a radiological or chemical exposure that exceeds the exposure standards defined in the SRD. Those features credited for the prevention of a criticality event are also designated as Safety Design Class.~~

~~Safety Design Significant SSCs are those needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that can, if they fail or malfunction, place frequent demands on, or adversely affect the function of, Safety Design Class SSCs.~~

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

24590-WTP-SRD-ESH-01-001-02, Appendix D, Radiological Exposure Standards for the RPP-WTP Project

Regulatory Basis

DOE/RL-96-0006	*3.3.1*	*Public Protection*
DOE/RL-96-0006	*3.3.2*	*Worker Protection*

Safety Criterion: 1.0 - 9

The RPP-WTP Contractor shall accept responsibility for the safety of the RPP-WTP.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Chapter: 1.0 Project Safety Approach
Section: 11.1 Design and Construction Phase
Section: 11.2 Operations Phase

Regulatory Basis

DOE/RL-96-0006	*4.1.2.1*	*Safety Responsibility-Safety Responsibility*
DOE/RL-96-0006	*4.3.1.1*	*Conduct of Operations-Organizational Structure*
DOE/RL-96-0006	*5.1.3*	*Process Safety Responsibility*

Safety Criterion: 1.0 - 10

In addition to the Safety Criteria contained herein, compliance with all requirements of 10 CFR 830.120 and 10 CFR 835 shall be achieved absent the granting of an exemption request to any specific requirement therein.

Regulatory Basis

10 CFR 830.120 Quality assurance requirements Location
10 CFR 835 Occupational Radiation Protection Location: 1
DE-AC06-96RL13308 Part I Section C.5 Table S4-1

SSCs that are designated Safety Design Class (excepting those so designated based solely on chemical hazards) and that are required to perform a safety function as a result of a given NPH shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. These SSCs are designated Seismic Category I (SC-I) for earthquakes and Performance Category 3 (PC-3) for other NPH. SSCs designated as Safety Design Class based solely on a safety function relative to chemical hazards shall be designated as SC-III for earthquakes, and shall be designed to meet PC-3 requirements for other NPH events.

SSCs that are designated Safety Design Significant whose continued function is not required for an NPH event, but whose failure as a result of an NPH event could reduce the functioning of a Safety Design Class SSC such that exposure standards might be exceeded, shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. For these SSCs, however, for seismic response only, credit may be taken for inelastic energy absorption per Table 2-4 of DOE-STD-1020-94. These SSCs are designated SC-II for earthquakes and PC-3 for other NPH. SSCs designated as Safety Design Significant based solely on a safety function relative to chemical hazards shall be designated as SC-III for earthquakes, and shall be designed to meet PC-3 requirements for other NPH events.

For any SSC included under this criterion, other NPH loads (for which the SSC has no safety function) may be taken from Safety Criterion 4.1-4 and Table 4-2 in lieu of Safety Criterion 4.1-3 and Table 4-1. SSCs designated as Safety Design Significant based solely on safeguarding a safety function relative to chemical hazards shall be designated SC-III for earthquakes, and shall be deisgned to meet PC-2 requirements for other NPH events.

Table 4-1. Natural Phenomena Design Loads for ~~Important to Safety~~SDC/SDS SSCs with NPH Safety Functions

Hazard	Load	Source Document for Load
Seismic	DBE with 0.26 *g* horizontal PGA and 0.18 *g* vertical PGA See Figures 4-1 and 4-2	WHC-SD-W236A-TI-002 [a] DOE-STD-1020-94[b]
Straight wind	111 mi/hr , 3-second gust, at 33 ft above ground, Importance factor, I=1.0	DOE Newsletter [c]
Wind Missile	2x4 timber plank, 15 lb at 50 mi/hr (horiz), Max height 30 ft	DOE-STD-1020-94 [b]
Tornado and Tornado Missiles	Not Applicable	DOE-STD-1020-94 [b]
Volcanic ash	12.5 lb/ft^2	HNF-SD-GN-ER-501 [d]
Flooding	Dry site for river flooding Local precipitation: 4 in. for 6 hours	HNF-SD-GN-ER-501 [d]
Snow	15.0 lb/ft^2 snow load	HNF-SD-GN-ER-501 [d]

[a] Geomatrix, 1996, *Probabilistic Seismic Hazard Analysis DOE Hanford Site, Washington,* WHC-SD-W236A-TI-002, Rev.1A, prepared for Westinghouse Hanford Company, Richland, Washington.

[b] DOE STD-1020-94, (1996, Change 1) *Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities*, U.S. Department of Energy, Washington, D.C., 1996.

[c] DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98.

[d] HNF-SD-GN-ER-501, Rev. 1, "Natural Phenomena Hazards, Hanford Site, South-Central Washington", Westinghouse Hanford Company.

Implementing Codes and Standards

ACI 349-97 Code Requirements for Nuclear Safety-Related Concrete Structures
ACI 349R-97 Commentary on Code Requirements for Nuclear Safety-Related Concrete Structures
ANSI/AISC N690-94 Specification for the Design, Fabrication, and Erection of Steel Safety-Related Structures for Nuclear Facilities
ASCE 4-98 (Draft) Seismic Analysis of Safety-Related Nuclear Structures and Commentary
ASCE 7-95 Minimum Design Loads for Buildings and Other Structures
DOE-STD 1020-94 (Change 1, 1996) Natural Phenomena Hazards Design and Evaluation Criteria for Department of Energy Facilities
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
1997 UBC Uniform Building Code
DOE Newsletter (Interim Advisory on Straight Winds and Tornados) Dated 1/22/98
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Regulatory Basis

DOE/RL-96-0006 4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure

---

Safety Criterion: 4.1 - 4

This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) without NPH safety functions. This criterion also addresses NPH design for SSCs with an NPH safety function ~~required~~ associated solely ~~to~~ with protection of workers and members of the public from exposure to chemical hazards ~~with an NPH safety function~~.

SSCs that may be important to the safety of the RPP-WTP shall be designed to withstand the effects of NPH such as earthquakes, wind, and floods. The SSCs included under this criterion are:

1. ~~SSCs Important to Safety (either~~ Safety Design Class (SDC) ~~or~~ and Safety Design Significant~~)~~ (SDS) SSCs that do not have an NPH safety function,

2. SSCs that have a seismic safety function solely because they protect workers and members of the public from exposure to chemical hazards,

~~2.~~3. Risk Reduction Class (RRC) SSCs ~~that are not Important to Safety and~~ that provide primary confinement of~~have~~ significant inventories of radioactive ~~or hazardous~~ materials but in amounts less than quantities that ~~might lead to~~require an SDC or SDS~~Important to Safety~~ designation, and ~~and~~

~~3.SSCs that are important to safety because of their function to protect workers and members of the public from exposure to chemical hazards.~~

4. ~~SSCs~~ RRC SSCs that ~~have been designated as RRC~~do not provide primary confinement of significant inventories of radioactive materials.

~~These~~ SSCs included under items 1, 2, or 3 (above) are designated Seismic Category III (SC-III) for earthquakes and Performance Category 2 (PC-2) for other NPH, and~~.SSCs included under this criterion~~ shall be designed to withstand the NPH loadings as provided in Table 4-2. ~~-~~SSCs designated as RRC that do not provide primary confinement of significant inventories of radioactive materials under item 4 ~~(~~above~~)~~ shall be designated Seismic Category IV (SC-IV) for earthquakes and Performance Category 1 (PC-1) for other NPH, in accordance with the PC-1 requirements of DOE-STD-1020-94. ~~SSCs designated as RRC under item 4 (above) shall be designated as SC-III or PC-2, however, if their failure under relevant NPH loads would result in failure of another item itself required to withstand SC-III or PC-2 NPH loads.~~

4.2 Confinement Design

Safety Criterion: 4.2 - 1

The facility shall be designed to retain the radioactive and hazardous material through a conservatively designed confinement system for normal operations, anticipated operational occurrences, and accident conditions. The confinement system shall protect the worker and public from undue risk of releases such that the radiological and chemical exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3
DOE Order 420.1 Facility Safety, 4.1.1.2

Regulatory Basis

DOE/RL-96-0006 *4.1.1.4 Defense in Depth-Mitigation*

Safety Criterion: 4.2 - 2

Important to Safety liquid and gaseous systems and components, including pressure vessels, tanks, heat exchangers, piping, and valves, shall be designed to retain their hazardous inventory such that the radiological and chemical worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.

Implementing Codes and Standards

ASME B31.3-96 Process Piping
ASME SEC VIII Boiler and Pressure Vessel Codes, Rules for Construction of Pressure Vessels
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

---

Safety Criterion: 4.2 - 3

Codes and standards for Important to Safety vessels and piping should be supplemented by additional measures (such as erosion/corrosion programs and piping in-service inspections) to mitigate conditions arising that could lead to a release of radiological or chemical material that would exceed the worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification
24590-WTP-SRD-ESH-01-001-02, Appendix E, Reliability, Availability, Maintainability, and Inspectability (RAMI)
Document P001/2 Rules for the Design of Piping Systems
Document V001/2 Rules for the Design of Vessels

Regulatory Basis

DOE/RL-96-0006 *4.2.2.2 Proven Engineering Practice/Margins-Common-Mode/Common-Cause Failure*

Safety Criterion: 4.2 - 4

Liquid and gaseous storage systems designated as Important to Safety shall have continuous monitoring to detect the loss or degradation of their safe storage function. As appropriate the following shall be monitored:

1. temperature; pressure; radioactivity in ventilation exhaust and liquid effluent streams
2. liquid levels
3. tank chemistry; condensate and cooling water
4. generation of flammable and explosive mixtures of gases

Implementing Codes and Standards

ANSI N42.18-1980 (Rev 1991) Specification and Performance of On-Site Instrumentation for Continuously Monitoring Radioactivity in Effluents [SDC or SDS]

ISA S84.01-1996, Application of Safety Instrumented Systems for the Process Industries [SDC or SDS]

ISA S12.13 PT 1-95 Performance Requirements, Combustible Gas Detectors [SDC or SDS]

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification [SDC, SDS or RRC]

4.3 Engineered Safety Systems

Safety Criterion: 4.3 - 1

Engineered safety systems shall be designed (1) to initiate automatically the operation of appropriate systems to assure that specified acceptable design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of Important to Safety systems and components. The ability to manually initiate engineered safety systems shall be provided.

Implementing Codes and Standards

ANSI/ANS 58.8-1994 Time Response Design Criteria for Safety-Related Operator Actions [SDC or SDS]
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth [SDC, SDS ~~& RRC~~or RRC]
ISA S84.01-96 Application of Safety Instrumented Systems for the Process Industries [SDC or SDS]
24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification [SDC, SDS ~~& RRC~~or RRC]

Regulatory Basis

DOE/RL-96-0006 *4.1.1.5 Defense in Depth-Automatic Systems*

Safety Criterion: 4.3 - 2

When single failure protection is required, Important to Safety engineered safety systems shall be designed to assure that the effects of natural phenomena (including lightning), and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth
IEEE 323-83 Qualifying Class 1E Equipment for Nuclear Power Generating Stations
IEEE 344-1987 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations
IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems
IEEE 384-1992 Standard Criteria for Independence of Class 1E Equipment and Circuits
NFPA 780-95 Standard for the Installation of Lightning Protection Systems
NFPA 801-95 Standard for Facilities Handling Radioactive Materials

Safety Criterion: 4.3 - 3

Important to Safety engineered safety systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Design provisions should be included to limit the loss of safety functions due to damage to several structures, systems, or components Important to Safety resulting from a common-cause or common-mode failure.

The protection system shall be designed to permit periodic testing of its functioning when the facility is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

Implementing Codes and Standards

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems [SDC or SDS]

IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems [SDC or SDS]

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification [SDC, SDS ~~& RRC~~or RRC]

Regulatory Basis

DOE/RL-96-0006 *4.2.2.2 Proven Engineering Practices/Margins-Common-Mode/Common-Cause Failure*

Safety Criterion: 4.3 - 4

Important to Safety instrumentation and controls shall be provided to monitor variables and systems and control systems and components over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate public and worker safety by compliance to the standards of Safety Criteria 2.0-1 and 2.0-2, including those variables and systems that can affect the performance of Important to Safety facility conditions. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. The instrumentation and controls provided shall provide the ability to detect off normal conditions, mitigate accidents, and place the facility in a safe state.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth [SDC, SDS ~~& RRC~~or RRC]

DOE IG Implementation Guide for Nonreactor Nuclear Safety Design Criteria and Explosive Safety Criteria, 2.3 [SDC or SDS]

DOE Order 420.1 Facility Safety, 4.1.1.2 [SDC or SDS]

ISA S84.01-96 Application of Safety Instrumented Systems for the Process Industries [SDC or SDS]

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification [SDC, SDS ~~& RRC~~or RRC]

Regulatory Basis

DOE/RL-96-0006 *4.1.1.3 Defense in Depth-Control*
DOE/RL-96-0006 *4.2.6.2 Human Factors-Instrumentation and Control Design*

4.4 Electrical and Mechanical Systems

Safety Criterion: 4.4 - 1

A list of electric and mechanical components designated as Important to Safety shall be prepared and maintained. The list shall include:

(1) The performance specifications for normal operation and under conditions existing during and following accidents.

(2) The load, pressure, voltage, frequency, and other characteristics, as appropriate, for which the performance specified can be ensured.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification

Safety Criterion: 4.4 - 2

Structures, systems, and components Important to Safety shall be designed and qualified to function as intended in the environments associated with the events for which they are intended to respond. The effects of aging on normal and abnormal functioning shall be considered in design and qualification.

Implementing Codes and Standards

10 CFR 50.49 Environmental qualification of electric equipment important to safety for nuclear power [SDC or SDS]

IEEE 323-83 Qualifying Class 1E Equipment for Nuclear Power Generating Stations [SDC or SDS]

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification [SDC, SDS ~~& RRC~~or RRC]

Regulatory Basis

DOE/RL-96-0006 *4.2.2.3 Proven Engineering Practices/Margins-Safety System Design and Qualification*

Safety Criterion: 4.4 - 3

This Criterion has been deleted.

Safety Criterion: 4.4 - 4

Structures, systems, and components Important to Safety shall be designated, designed and constructed to permit appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin.

Systems and components designated as Important to Safety that are located in closed cells where access is not possible during facility operation or scheduled shutdown periods shall be designed and constructed to standards aimed at ensuring their suitability for the entire service life with an adequate safety margin. Alternately, provisions may be made for remote replacement, standby cells, or equipment or other methods capable of ensuring a serviceable facility with adequate safety for the duration of the intended operating life.

Implementing Codes and Standards

24590-WTP-SRD-ESH-01-001-02, Appendix A, Implementing Standard for Safety Standards and Requirements Identification [SDC, SDS ~~& RRC~~or RRC]

24590-WTP-SRD-ESH-01-001-02, Appendix E, Reliability, Availability, Maintainability, and Inspectability (RAMI) [SDC, SDS ~~& RRC~~or RRC]

IEEE 338-1987 Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems [SDC or SDS]

ISA S84.01-1996, Application of Safety Instrumented Systems for the Process Industries [SDC or SDS]

Regulatory Basis

DOE/RL-96-0006 4.2.7.1 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Reliability

DOE/RL-96-0006 4.2.7.2 Reliability, Availability, Maintainability, and Inspectability (RAMI)-Availability, Maintainability, and Inspectability

Safety Criterion: 4.4 - 5

Each air treatment system designated as Safety Design Class shall have suitable redundancy in components and features, and suitable interconnections, leak detection, isolation, and confinement capabilities to ensure that for onsite electric power system operation (assuming offsite power is not available) and for offsite electric power system operation (assuming onsite power is not available) its safety function can be accomplished, assuming a single failure.

The use of alternate equipment may be considered to satisfy the single failure requirement.

Implementing Codes and Standards

IEEE 379-1994 Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems

ISA S84.01-1996, Application of Safety Instrumented Systems for the Process Industries

Safety Criterion: 6.0 - 4

During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components designated as Important to Safety shall be determined and documented. Operating points shall be adjusted to conform to values in the design basis. Training procedures and ~~l~~Limiting ~~c~~Conditions for ~~o~~Operation (when provided) shall be modified, if necessary, to accurately reflect the operating characteristics of the systems and components as built.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 3.14 Startup Testing and Operation
Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 *4.2.8.4* *Pre-Operational Testing-Design Operating Characteristics*

Safety Criterion: 6.0 - 5

A pre-startup safety review shall be performed. The pre-startup safety review shall confirm that, prior to the introduction of radioactive or process chemicals considered to pose a hazard to a process, construction and equipment is in accordance with design specifications; safety, operating, maintenance, and emergency procedures are in place and are adequate; a process hazard analysis has been performed and recommendations have been resolved or implemented before startup; and training of each employee involved in operating a process has been completed.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 5.6.4 Startup Review

Regulatory Basis

DOE/RL-96-0006 *4.3.1.4* *Conduct of Operations-Readiness*
DOE/RL-96-0006 5.2.6 Pre-startup Safety Review

7.0 Management and Operations

Safety Criterion: 7.0 - 1

Normal operations shall be conducted in accordance with approved operational safety requirements and in strict accordance with administrative and procedural controls.

Implementing Codes and Standards
24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.13 Procedures
Section: 5.6.1 Procedure Development

Regulatory Basis
DOE/RL-96-0006 4.3.1.2 Conduct of Operations-Normal Operations
DOE/RL-96-0006 5.1.3 Process Safety Responsibility

Safety Criterion: 7.0 - 2

Normal operation, including anticipated operational occurrences, maintenance, and testing, shall be controlled so that facility and system variables remain within their normal operating ranges and the frequency of demands placed on Important to Safety structures, systems, and components are small.

Implementing Codes and Standards
24590-WTP-SRD-ESH-01-001-02, Appendix B, Implementing Standard for Defense in Depth

Regulatory Basis
DOE/RL-96-0006 4.1.1.3 Defense in Depth-Control

Safety Criterion: 7.0 - 3

The operating organizations shall become and remain familiar with the features and limitations of components included in the design of the facility. They shall obtain appropriate input from the design organization on pre-operational testing, operating procedures, and the planning and conduct of training.

Implementing Codes and Standards
24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 1.3.14 Startup Testing
Section: 1.3.15 Operations

Regulatory Basis
DOE/RL-96-0006 4.1.5.2 Configuration Management-Contractor Design Knowledge

7.4 Unreviewed Safety Questions

Safety Criterion: 7.4 - 1

A safety evaluation shall be performed to determine whether a situation involves an unreviewed safety question (USQ) for:

(1) Temporary or permanent changes in the facility as described in the existing authorization basis

(2) Temporary or permanent changes in the procedures as derived from existing authorization basis

(3) Tests or experiments not described in the existing authorization basis

A situation involves a USQ if:

1) the probability of occurrence or the radiological or chemical consequences of an accident or malfunction of equipment ~~Important to Safety~~designated as SDC or SDS, previously evaluated in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility analysis, may be increased

2) a possibility for an accident or equipment malfunction of a different type than any evaluated previously in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility safety analysis, may be created

3) any margin of safety is reduced

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Regulatory Basis

DOE/RL-96-0006	*4.4.4*	*Unresolved Safety Questions*
DOE/RL-96-0006	*5.2.9*	*Management of Change*

Safety Criterion: 7.4 - 2

Regulatory approval shall be obtained for situations determined to involve an unreviewed safety question or a change in a technical safety requirement, prior to initiating the activity, if the initiation of the activity would itself involve a USQ, or implementing the proposed change.

Implementing Codes and Standards

24590-WTP-ISMP-ESH-01-001, Integrated Safety Management Plan
Section: 3.16.4 Unreviewed Safety Questions

Regulatory Basis

DOE/RL-96-0006	*4.4.4*	*Unresolved Safety Questions*

11.0 Definitions

Credible event: Any event with a frequency greater than 10^{-6} per year, including allowance for uncertainties.

Important to Safety: Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related, or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related, may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition. The WTP has divided Important to Safety items into three separate categories: Safety Design Class, Safety Design Significant, and ~~RRC~~Risk Reduction Class, as defined in Safety Criterion 1.0-8.

Mitigated event: As used in this standard, a mitigated event involves the following sequence:

- An initiating event that could lead to a release from the primary confinement barrier
- Failure of all elements of the control strategy that would prevent the initiating event from developing into a release from the primary confinement barrier
- Mitigation of the consequences of the release as provided by the control strategy

Mitigated event frequency: The mitigated event frequency is the corresponding release frequency times the probability that the elements of the control strategy that mitigate the release will function given the release.

Release frequency: The release frequency is the product of the frequency of the initiating event times the probability that all elements of the control strategy that would prevent the release fail, given the initiating event.

Reliability: The probability that an SSC will perform its safety function when required.

Appendix B: Implementing Standard for Defense in Depth

Conceptually, there are three levels of defense in depth.

1. The first level of defense consists of a well-designed facility with process design to reduce source terms, reliable SSCs that are simple to operate and maintain and resistant to degradation, and personnel well trained in operations and maintenance and committed to a strong safety culture.
2. The second level recognizes that failures of systems and components and human failures cannot be entirely eliminated and that protective features (e.g., engineering design features and administrative controls) are required. These Risk Reduction Class features are provided to ensure a return to normal operation or to bring the facility to a safe condition in the event of anticipated, but abnormal events. These features may provide automatic system response to such events or may be monitors that alert operators to the necessity of taking manual action. Such response to off-normal conditions can effectively halt the progression of events toward an accident.
3. The final level of defense consists of conservatively designed ~~*important to* safety~~Safety Design Class or Safety Design Significant SSCs to prevent or mitigate the consequences of accidents that may be caused by errors, malfunctions, or events that occur both internal and external to the facility (Ref. 5.3).

Implementing Standards for the following elements of defense in depth described in the nonreactor safety Implementation Guide (IG) related to safety design and construction are addressed in the sections of this document that are referenced below.

IG Element	Discussed in Section
Siting	2.2.2
Material at risk	2.2.2
Conservative design	2.2.2
Quality assurance	2.6.2
Physical barriers	2.4.2
Critical safety functions	2.3.2
Equipment and administrative controls	2.3.2 and 2.6.1
Emergency features	2.5.2

When active SSCs are required to achieve defense in depth, RPP-WTP will apply the single failure criterion in accordance with ANSI/ANS-58.9 (Ref. 5.8) for fluid systems and IEEE Std 379 (Ref. 5.9) for electrical and instrumentation and control systems, as discussed below.

External Event. An event external to the RPP-WTP caused by (1) a natural hazard (e.g., earthquake, flood, lightning, or range fire) or (2) a human-induced event (e.g., transportation or nearby industrial activity).

Human factors engineering (HFE). An interdisciplinary science and technology concerned with the process of designing for human use (Ref. 5.12).

Important to Safety. Structures, systems and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily explicitly) in the top-level radiological nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation).

This definition includes not only those structures, systems and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems and components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems and components should be considered for inclusion within this definition (Ref. 5.4). The WTP has divided Important to Safety items into three separate categories: Safety Design Class, Safety Design Significant, and Risk Reduction Class.

Independence. The state in which there is no mechanism by which any single design basis event, such as a flood, can cause redundant equipment to be inoperable (Ref. 5.10).

Initiating occurrence/event. A single occurrence and its consequential effects that place the plant or some portion of the plant in an off-normal condition. An initiating occurrence/event is not the single failure defined elsewhere herein. An initiating occurrence can be *an internal event or an external event* (Ref. 5.5, 5.6, 5.8).

The first event in an event sequence. Can result in an accident unless engineered protection systems or human actions intervene to prevent or mitigate the accident (Ref. 5.15).

Internal Event. An occurrence related to structure, system, and component performance or human action, or an occurrence external to the system but within the RPP-WTP that causes upset of a structure, system, or component.

Shall [be] consider[ed]. An objective assessment must be performed to determine the extent to which the single failure criterion will be incorporated into or be satisfied by design. The results and basis of this assessment shall be documented. Such documentation shall be retrievable and can be in the form of engineering studies, meeting minutes, reports, internal memoranda, etc. (Ref. 5.16).

Short term. *For fluid systems*, the short term is defined as that period of operation up to 24 hours following an initiating event [ ] (Ref. 5.8).

Single failure. A random failure and its consequential effects, in addition to an initiating occurrence, that result in the loss of capability of a component to perform its intended [ ] safety function(s) (Ref. 5.5, 5.6).

Single failure criterion. [Two definitions are provided below. The following definition applies to fluid (i.e., liquid and gas) systems.]

> Fluid [ ] systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly), nor (2) a single failure of any passive component (assuming active components function properly) results in a loss of the capability of the system to perform its [ ] safety function (Ref. 5.5, 5.6).

[The following statement of the "single failure criterion" applies to electrical and instrumentation and control systems.]

> When required, ~~T~~the *important to* safety systems shall perform all required safety functions for a design basis event in the presence of the following:

1. Any single detectable failure within the *important to* safety systems concurrent with all identifiable but non-detectable failures
2. All failures caused by the single failure
3. All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function

> The single failure could occur prior to, or at any time during, the design basis event for which the *important to* safety system is required to function (Ref. 5.9).

6.0 Tailoring of Consensus Standards Used in the Implementing Standard for Defense in Depth

The following subsections summarize the RPP-WTP contractor's tailoring of the consensus standards invoked by this Implementing Standard for Defense in Depth.

6.1 DOE O 420.1, Facility Safety (Ref. 5.2)

Terminology

- Section 4.1.1.2, 1st paragraph, last sentence: Phrase "…workers, including those at adjacent facilities…" is interpreted for RPP-WTP to mean "…workers and collocated workers…"

Applicability

- The only portion of DOE O 420.1 that is being invoked by this Implementing Standard for Defense in Depth is Section 4.1.1.2, the first three paragraphs.

6.2 Implementation Guide for Nonreactor Nuclear Safety Criteria and Explosives Safety Criteria (Ref. 5.3)

Terminology

- By virtue of cross-references within the DOE Implementation Guide (IG), reference is made to "safety class" and "safety significant" SSCs. The RPP-WTP project uses the term "safety design class and safety design significant~~important to safety~~", which encompasses both "safety class" and "safety significant".
- "Critical safety function" in the DOE IG is interpreted to more broadly read "…significant public, worker and collocated worker impact".

Applicability

- The only portion of the DOE "420.X" Implementation Guide that is being invoked by this Implementing Standard for Defense in Depth is Section 2.3, except the last paragraph.
- Section 2.3 of the DOE IG contains internal cross-references to subsections 5.2.1, 5.2.2.1 and 5.2.2.2, which list typical codes for structures, ventilation systems, and process equipment that provide a confinement function. Section 2.4.2 of this Implementing Standard lists the SRD Safety Criteria that will be applied to SSCs comprising confinement.
- Section 2.3 of the DOE IG contains an internal cross-reference to subsection 5.2.1, which further cites section 4.4 of DOE O 420.1 and section 3.3 of the DOE IG for criteria for natural phenomena hazards (NPH). For the RPP-WTP, NPH criteria are provided in SRD Safety Criteria SC 4.1-3 and SC 4.1-4.

6.3 ANSI/ANS-58.8-1994, Time Response Design Criteria for Safety-Related Operator Actions (Ref. 5.7)

Terminology

- "Safety-related" is interpreted for RPP-WTP to mean "SDC or SDS~~important to safety~~" ~~or "ITS"~~.
- "Safety-related function" is interpreted for RPP-WTP to mean "safety function needed to ensure radiological exposures to worker or members of the public do not exceed appropriate limits" as defined in DOE/RL-96-0006, Rev. 1.

Non-Applicability

- Assumption (1) of section 1.3 does not apply. Single failure criteria for the RPP-WTP project are given in the consensus standards invoked and tailored by this Implementing Standard (ANSI/ANS-58.9-1981 and IEEE 379-1994).
- Assumption (4) of section 1.3 does not apply. The operators will be qualified in accordance with the RPP-WTP training program, per Safety Requirements Document Volume II (24590-WTP-SRD-ESH-01-001-02), Section 7.2.
- "Automatic reactor trip…" does not apply.

6.4 ANSI/ANS-58.9-1981, Single Failure Criteria for Light Water Reactor Safety-Related Fluid Systems (Ref. 5.8)

Terminology

- "Containment" or "containment vessel" is interpreted to mean "confinement".
- "Seismic Category I standards" is interpreted as seismic requirements for a SSC with a seismic safety function per SRD Volume II (24590-WTP-SRD-ESH-01-001-02) Safety Criterion 4.1-3 for the RPP-WTP.
- "Safety related" is interpreted for RPP-WTP to mean "SDC or SDS~~important to safety~~" ~~or "ITS"~~. Conversely, "non-safety-related" means "non-ITS".
- "Technical specification(s)" is interpreted to mean "Technical Safety Requirements" or "TSR(s)".
- "Condition I" is interpreted for RPP-WTP to mean "normal operation".
- "Safety-related function" is interpreted for RPP-WTP to mean "safety function" as defined in DOE/RL-96-0006, Rev. 1.
- In definition of "single failure", reference [1] does not apply to RPP-WTP.

Safety classes 1, 2, and 3 (section 4.5) are interpreted to be SDC or SDS~~important to safety~~ systems.

Non-Applicability

- For RPP-WTP, the need for emergency onsite power will be ascertained in accordance with the DOE/RL-96-0004 process as part of determining hazard control strategies.
- In the definition of "short term" (section 2), everything after "…up to 24 hours following an initiating event" applies to nuclear power reactor plants and is therefore not applicable to RPP-WTP.
- Sections 3.1 through 3.3 of ANSI/ANS 58.9 are not applicable to the RPP-WTP. Applicability of the single failure criteria to the work and hazards presented by the RPP-WTP is described in Section 3.0 of this Implementing Standard.
- Reactor-specific regulations (e.g., 10 CFR 50 Appendix A) are not applicable to RPP-WTP (see Section 1, 1st paragraph).
- References to a reactor "unit", "safe shutdown", and "loss of coolant accident" are nuclear reactor plant-specific and, therefore, do not apply to RPP-WTP.
- Sections 3.1 through 3.3 are reactor-specific and do not apply to RPP-WTP.

6.5 IEEE STD 379-1994, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (Ref. 5.9)

Terminology

- BNI uses the definitions of the following terms given in DOE/RL-96-0006, rather than those in section 3 of the consensus standard:

– Common-cause failure

– Design basis events

– Safety function

- "Safety system" is interpreted for RPP-WTP to mean an "SDC or SDS~~important to safety~~ system"~~. Consequently, "important to safety system" is interpreted to mean a system~~ that performs a safety function needed to ensure radiological exposures to worker or members of the public do not exceed appropriate limits, as defined in DOE/RL-96-0006.
- "Containment" or "containment vessel" is interpreted to mean "confinement" for the RPP-WTP.

Applicability

- Applicability of the single failure criteria to the work and hazards presented by the RPP-WTP is described in Section 3.0 of this Implementing Standard.
- Nuclear reactor plant-specific terms such as reactor "unit", "reactor trip system" power, control rods, "safety injection", "core spray", and "low pressure coolant injection" do not apply to RPP-WTP.

~~6.6 IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (Ref. 5.11)~~

~~**Terminology**~~

- ~~The definition of "administrative controls" in section 2 of the consensus standard is understood as being consistent with the definition given in section 4.0 of this Implementing Standard.~~
- ~~The definition of "Class 1E" is interpreted for the RPP-WTP as follows: "The classification of the electric equipment and systems that perform a safety function." The note following the definition of "Class 1E" in the consensus standard is retained for RPP-WTP.~~
- ~~BNI uses the definitions of the following terms given in DOE/RL-96-0006, rather than those in section 3 of the consensus standard:~~
  - ~~Design basis events~~
  - ~~Safety function~~
- ~~"Safety system" is interpreted for RPP-WTP to mean "SDC or SDSimportant to safety system". Consequently, "SDC or SDSimportant to safety system" is interpreted to mean a system that performs a safety function needed to ensure radiological exposures to worker or members of the public do not exceed appropriate limits, as defined in DOE/RL-96-0006.~~
- ~~"Containment" or "containment vessel" is interpreted to mean "confinement" for the RPP-WTP.~~
- ~~"Nuclear power generating stations" is interpreted to mean a nuclear facility such as RPP-WTP.~~

~~**Non-Applicability**~~

- ~~Nuclear reactor plant-specific terms such as reactor "unit", "emergency reactor shutdown", "reactor heat removal", do not apply to RPP-WTP.~~

6.7 IEEE STD 1023-1988, IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations (Ref. 5.12)

Terminology

- "Nuclear power generating stations" is interpreted to mean a nuclear facility such as RPP-WTP.

Non-Applicability

- Application of the formal human factors engineering process described in subsection 6.1.1 of IEEE Std 1023-1988 is tailored to the work and hazards presented by the RPP-WTP in subsection 2.6.2 of this Implementing Standard.

- Section 6.1.1.12 and 6.1.1.18 of IEEE Standard 1023-1998 recommends the use of a separate plant simulator or physical mockup for human factors engineering. As discussed in subsection 2.6.2 of this Implementing Standard, the RPP-WTP contractor does not currently plan to construct a separate plant simulator or physical mockup and these sections are, therefore, not applicable to RPP-WTP.

6.8 ISA-S84.01-1996, Safety Instrumented Systems for the Process Industries (Ref. 5.13)

Terminology

- The definition of "common-cause failure" given in DOE/RL-96-0006 is used, rather than that in section 3 of the consensus standard.
- "Safety Instrumented System (SIS)" is interpreted to refer to any instrumentation and control system in the RPP-WTP that is SDC or SDS~~important to safety, as defined in DOE/RL-96-0006~~.

Appendix C: Implementing Standards

4.0 DOE G-420.1/G-440.1, Implementation Guide for Use with DOE Orders 420.1 and 440.1, Fire Safety Program*

Revision: September 30, 1995

Sponsoring Organization: U. S. Department of Energy

RPP-WTP Specific Tailoring

The following tailoring of DOE G-420.1/G-440.1 is required for use by the RPP-WTP Project as an implementing standard for fire safety.

Section III.5.0

Add the following words at the end of the paragraph: "The applicable building code for the RPP-WTP Project is the 1997 Uniform Building Code (UBC)."

Justification: To clarify that the code in effect at the time that facility design commenced was the 1997 UBC.

Section III.6.3

Revise to read "Automatic fire extinguishing systems in all areas subject to loss of safety class systems, significant life safety hazards, or unacceptable program interruption. The FHA may justify the omission of such systems based on safety considerations as approved by the AHJ.

Justification: The addition is consistent with governing Safety Criterion 4.5-4, which requires automatic fire suppression "unless the Fire Hazards Analysis dictates otherwise". It is also consistent with the DOE equivalency concept described in DOE G-420.1/G-440.1 Section II.

Section IV.4.5

Change "Description of critical process equipment" to "Identification of Important-To-Safety ~~(i.e.,~~ SDC or SDS~~)~~ Equipment".

Justification: The term "critical process equipment" is not well defined for the RPP-WTP Project. By contrast the term "Important-to-Safety" is defined by the DOE regulatory documents, such as DOE/RL-96-0004. Identification of Important-to-Safety equipment is more meaningful and is consistent with the CAR Guidance (RL/REG-99-05). The Safety Design Class (SDC) and Safety Design Significant (SDS) categories of Important to Safety SSCs constitute those SSCs that are specifically credited in the control strategies for postulated accidents and are thus analogous to "critical process equipment."

SSCs designated~~defined~~ as Important-to-Safety for the RPP-WTP include the ~~following~~Safety Design Class, Safety Design Significant, and Risk Reduction Class, as defined in SRD SC 1.0-8.

1) SSCs needed to prevent or mitigate accidents that could exceed public or worker radiological and chemical exposure standards of Table 1-2 and SSCs needed to prevent criticality. This set of SSCs includes both the front line and support systems needed to meet these exposure standards or to prevent criticality. This set of Important-to-Safety SSCs are designated as Safety Design Class.
2) SSCs needed to achieve compliance with the radiological or chemical exposure standards for the public and workers during normal operation; and SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction. This set of Important-to-Safety SSCs are designated as Safety Design Significant.

The processes for identifying the SSCs for each of the ~~two~~ groups of SSCs Important-to-Safety and the requirements assigned to each of the ~~two~~ groups are discussed below.

Safety Design Class SSCs typically are identified by the results of accident analyses that show the potential for exposure standards to be exceeded. However, additional items also are designated Safety Design Class independent of a specific accident analysis. These are items that protect the facility worker from potentially serious events. Typically, these events are deemed to present a challenge to the facility worker severe enough that mitigation is prudent, without the need to perform a specific consequence analysis. These latter items are identified by the results of the HAR.

Safety Design Significant SSCs are identified in several ways including: (1) SSCs identified as significant contributors to safety by the risk analyses that confirm the facility accident risk goals are met (this is one way to identify SSCs that place frequent demands on, or adversely affect the function of, Safety Design Class SSCs if they fail or malfunction), (2) SSCs that are needed to ensure that standards for normal operation are not exceeded (e.g., bulk shield walls or radiation monitors), (3) SSCs selected based on the dictates of nuclear and chemical facility experience and prudent engineering practices, and (4) SSCs whose failure could prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items).

SSCs identified in ISAR Section 4.8, "Controls for Prevention and Mitigation of Accidents" as Design Class I and II are Safety Design Class SSCs. SSCs provided to protect the health and safety of the public and collocated workers usually are considered to also provide adequate protection of the environment. As stated in ISAR Section 4.8, "The selection of engineered and administrative controls is based on the conceptual design of the facility. Additional or different features may be identified during Part B". The more complete group of Important-to-Safety SSCs will be identified in Part B and provided in the Preliminary Safety Analysis Report (PSAR) as part of the Construction Authorization Request. The PSAR and the Final Safety Analysis Report also will describe SSCs that are not designated as Important-to-Safety. The descriptions of these SSCs will note that they are not classified as Important-to-Safety.

When a SSC is classified as Safety Design Significant it ~~is~~ has the following attributes.

1) Quality Level 2 (QL-2) is applied to the SSC. The QAP describes the requirements associated with QL-2.

2) The SSC is designed to withstand the effects of natural phenomena such that it can perform its safety functions required as a result of a natural phenomena event. If an earthquake can produce exposures to the public or workers in excess of standards, the Safety Design Class SSC that prevents or mitigates the exposures would be designed DBE-resistant as discussed above. The same NPH loads also are applied to a Safety Design Significant SSC if failure of the item could prevent the Safety Design Class SSC from performing its safety function required as a result of the DBE. Such an SSC is designated Seismic Category II. It should be noted, however, that DBE resistance is not automatically applied to Safety Design Significant SSCs. It is applied only when the earthquake is the initiating event, or when the earthquake could cause the initiating event. A Safety Design Significant SSC that does not have a DBE mitigating function is designated Seismic Category III.

   This NPH design philosophy is used for all severe natural phenomena events (i.e., earthquake, flood, high wind). Therefore, if a Safety Design Significant SSC is needed to meet public or worker exposure standards for a given NPH event, the NPH loads associated with that event are taken from SRD Volume II, Table 4-1, "Natural Phenomena Design Loads for Important-to-Safety SSCs with NPH Safety Functions". All other NPH loads for the Safety Design Significant SSC may be taken from SRD Volume II, Table 4-2, "Natural Phenomena Design Loads for SSCs without NPH Safety Functions" in lieu of SRD Table 4-1.

3) General and specific design requirements are applied as identified in Section 4.0 of the SRD for Safety Design Significant SSCs.

4) Other design requirements again may be applied based on the specific safety function to be performed by the Safety Design Significant SSC.

When an SSC is classified as Risk Reduction Class (RRC),~~-~~ it ~~is~~ has the following attributes:

1) Commercial grade quality requirements, in accordance with QAM compliance with DOE Order 414.1A, are applied to the SSC. Requirements associated with Quality Affecting Software do not apply to RRC items.

2) The application of defense in depth is not required to preserve the safety function of an RRC SSC.

3) RRC SSCs are normally designed to Seismic Category IV requirements for earthquakes and PC-1 requirements for other natural phenomena hazards,~~.~~ ~~The~~ except~~ion~~ that RRC SSCs that provide primary confinement of significant amounts of radioactive materials, as illustrated in Table 1-3, are designed to Seismic Category III requirements for earthquakes and PC-2 requirements for other NPH.
   ~~to this would be cases in which the RRC item could fail under seismic loads in such a way as to cause failure of SDS or other RRC items. In these cases, if the SDS item is required to~~

~~remain functional after the seismic event, the RRC item would be designed to the same criteria as the affected SDS or RRC item.~~

4) An SSC, not designated as SDC or SDS, whose function is necessary to ensure the integrity of the boundaries retaining radioactive materials is classified as RRC when the SSC contains a significant quantity of radioactivity, as illustrated by Table 1-3.

5) An SSC, not designated as SDC or SDS, whose function is necessary to ensure the capability to place and maintain the facility in a safe state is classified as RRC. In this context, a facility is considered to be in a safe state when:
   - Process transfers involving significant quantities of radioactive or extremely hazardous materials have stopped and the material is contained in passive SSCs.
   - Process reactions that generate energy (e.g. heat, pressure) or flammable gasses are contained or controlled such that these byproducts do not pose a significant hazard.
   - The structures, systems, and components necessary to achieve and maintain these conditions are functioning in a stable manner, with relevant process parameters in their predetermined safe state ranges.

6) Design codes and standards for RRC SSCs will be selected in accordance with the process defined in SRD Volume II, Appendix A and will be (at a minimum) consistent with practices in the commercial radiological or chemical industries, as appropriate.~~RRC SSCs are normally designed to standard engineering requirements.~~

7) Other design requirements ~~again~~ may be applied based on the specific safety function to be performed by the RRC SSC. This specific safety function is determined by the ISM analysis that identified the need for the RRC SSC.

8) Unless specifically identified as needed through the DBE analyses, Technical Safety Requirements ~~s~~ are not applied to RRC SSCs.

9) Failure or degradation of an RRC SSC would not, in itself, generally lead to an Unusual Occurrence report.

10) The Unreviewed Safety Question determination (USQD) process evaluates changes to RRC SSCs in a similar fashion as for non-ITS SSCs. That is, changes to RRC items will be controlled through the AB change screening process to identify when they are modified. "Modifying" an RRC item, as the term is used here, is a change that would affect the performance of its RRC function as it is defined in the safety analysis report. Eliminating or modifying the function of an RRC item will not in itself require a USQ~~E~~D or result in a positive USQ. However, since eliminating or modifying an RRC control represents a change in commitment made in the AB, the DOE needs to be made aware of the change. Therefore, if a proposed activity is identified as impacting an RRC SSC or program requirement for implementing controls for an RRC SSC, then a copy of the documentation, clearly identifying the impact to the RRC control, shall be forwarded to the DOE for information.

11) Maintenance, operation and testing of RRC SSCs will be controlled in a similar fashion as for non-ITS SSCs. The configuration of RRC SSCs will be managed as part of the technical baseline, including replacement parts evaluation, setpoint control, and design change control.

12) Appropriate preventive and predictive maintenance will generally be applied to RRC equipment.

13) Monitoring of performance and condition and trending of the need for maintenance will also generally be applied to RRC SSCs. This monitoring and trending will provide input to the schedule and scope of the preventive and predictive maintenance and will also identify the need for replacement or modification of RRC SSCs.

Table 1-3
Illustration of Significant Amount of Radioactivity[1]

Vessel	Activity (Curies)	Facility Worker Dose (rem)	Co-located Worker Dose (rem)	Classification
LAW Concentrate Receipt Vessel	500	5.0	0.6	RRC
LAW Melter Feed Preparation Vessel	170	2.5	0.2	RRC
HLW Offgas Drains Collection Vessel	460	0.9	9.6E-3	RRC
LAW SBS Condensate Collection Vessel	0.5	0.03	0.02	NON
LAW SBS CondensateVessel	4.7	0.03	0.01	NON
LAW Submerged Bed Scrubber	1.1	0.03	2.5E-3	NON
HLW Decon Effluent Collection Vessel	0.7	1.4E-4	2.9E-5	NON

1.3.11 Quality Levels

The assignment of Quality Levels (QL) is the method by which the implementation of the graded quality approach discussed in 10 CFR 830.120, "Quality Assurance Requirements" is ensured. Designation of correct quality levels helps to ensure that the appropriate quality assurance requirements are applied to specific RPP-WTP SSCs. The quality levels of the Project quality assurance approach and their applications are described in the QAP.

1.3.12 Training

Training serves an important role in the Project by ensuring that the personnel involved with the project have sufficient knowledge to safely fulfill the roles and responsibilities of their assigned tasks. Training has a direct impact on safety during design, construction, operation, and deactivation of the project by:

1) Improving technical ability
2) Enhancing personal skills

[1] Values in the table are provided only to illustrate the concept of a significant amount of radioactivity; actual values are provided in the safety analysis report.

3) Increasing awareness of signs of potential hazardous situations in the workplace

SRD Proposed Changes Summary ~~/Safety~~ Evaluation [Note 1]

SRD Criterion	Proposed Change	Basis for AB impact assessment
1.0-8	Expanded SDC and SDS. Added definition of RRC.	Addition of the third (RRC) category ~~increases~~ enhances ~~the margin of~~ safety~~, lowers risk~~.
4.0-3	No change required - Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional RRC items.
4.1-2	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional RRC items.
4.1-3 Table 4-1	Change ITS to SDC/SDS	Change title to be consistent with the criteria citing the table. [Note 2]
4.1-4	Item 1: ~~delete~~ Replace "Important to Safety" to SDC and SDS. Reverse items 2 & 3 for clarity. ~~;~~ Item 2: Minor changes for clarity. Item 3: Changed non-ITS to RRC; reworded for clarity. ~~Change ITS to SDC/SDS; Item 3: leave as is;~~ Item 4 added for RRC~~.~~ SSCs that do not privide primary confinement of radioactivity.	As written the criterion applies only to SDC/SDS items. Revisions are needed to incorporate new ITS category of RRC. [Note 2]
4.1-6	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional RRC items.
4.2-2	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional RRC items.
4.2-3	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional RRC items.
4.2-4	Identified applicability of implementing standard to SDC, SDS or RRC. Added SRD Volume II, Appendix A as implementing standard for RRC. ~~Change ITS to SDC/SDS~~	Criteria and implementing standards as written are excessively conservative for RRC items. A less conservative implementing standard is needed to match RRC items to the Top Level Standard. ~~Criteria and implementing standards are excessively conservative for RRC items. Criteria is appropriate if limited to SDC/SDS items. [Note 2]~~
4.3-1	Identified applicability of implementing standard to SDC,	Criteria and implementing standards as written are excessively conservative for RRC items. A

SRD Proposed Changes Summary ~~/Safety~~ Evaluation [Note 1]

SRD Criterion	Proposed Change	Basis for AB impact assessment
	SDS or RRC. Added SRD Volume II, Appendix A as implementing standard for RRC.	less conservative implementing standard is needed to match RRC items to the Top Level Standard.
4.3-2	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
4.3-3	Change ITS to SDC/SDS. Identified applicability of implementing standard to SDC, SDS or RRC. Added SRD Volume II, Appendix A as implementing standard for RRC.	Criteria and implementing standards as written are excessively conservative for RRC items. A less conservative implementing standard is needed to match RRC items to the Top Level Standard. [Note 2]
4.3-4	Change ITS to SDC/SDS. Identified applicability of implementing standard to SDC, SDS or RRC. Added SRD Volume II, Appendix A as implementing standard for RRC.	Criteria and implementing standards as written are excessively conservative for RRC items. A less conservative implementing standard is needed to match RRC items to the Top Level Standard. [Note 2]
4.3-5	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
4.3-6	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
4.4-1	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
4.4-2	Identified applicability of implementing standard to SDC, SDS or RRC. Added SRD Volume II, Appendix A as implementing standard for RRC.	Criteria and implementing standards as written are excessively conservative for RRC items. A less conservative implementing standard is needed to match RRC items to the Top Level Standard. [Note 2]
4.4-4	Identified applicability of implementing standard to SDC, SDS or RRC.	Criteria and implementing standards as written are excessively conservative for RRC items. A less conservative implementing standard is needed to match RRC items to the Top Level Standard. [Note 2]
4.4-17	No change required -Criterion, implementing standards	Standards cited do not require tailoring to address additional, RRC items.

SRD Proposed Changes Summary ~~/Safety~~ Evaluation [Note 1]

SRD Criterion	Proposed Change	Basis for AB impact assessment
	adequate for RRC as written.	
6.0-1	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
6.0-3	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
6.0-4	Add "when provided" after "Limiting Conditions for Operation".	Change needed for clarification; not all ITS items (eg., RRC) will be associated with LCO's.
7.0-2	Add Appendix B as the implementing standard	Change needed to correct an earlier omission; Appendix B is the correct implementing standard for DiD.
7.4-1	Change ITS to SDC/SDS.	Criteria and implementing standards as written are excessively conservative for RRC items. A less conservative implementing standard is needed to match RRC items to the Top Level Standard. [Note 2]
7.6-2	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
7.6-3	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
Appendix A 6.0	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
11.0	Add SDS/SDC to definition of ITS.	Change added for clarification that WTP terms are included in ITS definition.
Appendix B 2.1.2	Add RRC to level 2 discussion, change ITS in level 3 discussion to SDC/SDS.	Change needed to clarify the relationships between SDC/ SDS, RRC items and the various levels of DiD.
Appendix B 2.3	Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
Appendix B 2.5.2	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
Appendix B 2.6.2	No change required -Criterion, implementing standards adequate for RRC as written.	Standards cited do not require tailoring to address additional, RRC items.
Appendix B 4.0	Add SDC, SDS, RRC to definition of ITS	Change added for clarification that WTP terms are included in ITS definition

SRD Proposed Changes Summary ~~/Safety~~ Evaluation [Note 1]

SRD Criterion	Proposed Change	Basis for AB impact assessment
Appendix B 4.0	Defense in depth definition, no change needed.	Definition effectively includes concept of RRC as written.
Appendix B 4.0	Definition of "Long Term", no change needed.	Definition effectively includes concept of RRC as written.
Appendix B 4.0	"Single Failure Criterion": Add "when required" to clarify applicability.	Change needed for clarification, single failure criterion does not apply to RRC items.
Appendix B 6.2	Changed ITS to SDC/SDS in "Terminology": clarify only applies to SDS/SDC items.	Change needed to clarify that the implementing standard's use of SDC/SDS does not incorporate concept of RRC. [Note 2]
Appendix B 6.3	Changed ITS to SDC/SDS in "Terminology": Change ITS to SDC/SDS items.	Change needed to clarify that the implementing standard's use of SDC/SDS does not incorporate concept of RRC. [Note 2]
Appendix B 6.4	Changed ITS to SDC/SDS in "Terminology": Change ITS to SDC/SDS items.	Change needed to clarify that the implementing standard's use of SDC/SDS does not incorporate concept of RRC. [Note 2]
Appendix B 6.5	Changed ITS to SDC/SDS in "Terminology": Change ITS to SDC/SDS items.	Change needed to clarify that the implementing standard's use of SDC/SDS does not incorporate concept of RRC. [Note 2]
Appendix B 6.8	Changed ITS to SDC/SDS in "Terminology": Change ITS to SDC/SDS items.	Change needed to clarify that the implementing standard's use of SDC/SDS does not incorporate concept of RRC. [Note 2]
Appendix C 4.0 IV.4.5	Change "Important to Safety" to "SDC/SDS"	Change needed to clarify that the implementing standard's use of SDC/SDS does not incorporate concept of RRC. [Note 2]

Note 1 – The rationale in determining the extent of the changes to the Safety Criterion dealing specifically with Important to Safety items was to, whenever possible, leave the criterion alone. That is, if it could be inferred fro~~r~~m the wording of the criterion that the requirements pertained to only a subset of the ITS item (e.g., single failure requirements)~~,~~; no change was recommended.

Note 2 – Since the function of SDC/SDS items is to protect individuals from significant radiological hazards (e.g., those that would exceed the ~~Release~~ Radiation Exposure Standards), it is appropriate~~d~~ to cite the more stringent or conservative design standards. However, RRC items are not required to meet the performance requirements for these SDC/~~-~~SDS items and thus the design standards cited may differ~~should be tailored~~.

Summary of ISM Process for Revision to Implementing Standards and Safety Criteria

1 Purpose

This attachment summarizes and documents the ISM process associated with the proposed changes contained within this ABCN.

2 Scope

This attachment is limited to a summary of the application of the ISM process that resulted in the changes associated with 24590-WTP-ABCN-ESH-01-029, Rev. 1. Attachments 1, 2 , and 3 of 24590-WTP-ABCN-ESH-01-029 document the actual proposed changes to the SRD and ISMP.

3 Discussion

3.1 Approach

The identification of the proposed changes to the SRD and ISMP were performed in compliance with project procedure 24590-WTP-GPP-SANA-002. The process consists of the following major steps:

- Initiate Process
- Identify Work
- Hazard Evaluation
- Development of Preferred Hazard Control Strategies
- Design Basis Events (DBEs)
- Designation of Systems Structures, and Components (SSCs) Comprising the Hazard Control Strategy
- Identification of Standards
- Confirmation of Standards
- Record Document Identification
- Documentation

These steps are discussed in more detail below.

3.2 Results

3.2.1 Initiate Process (ISM Team Composition)

Project procedure 24590-WTP-GPP-SANA-002, Section 3.10, Identification of Standards states: "Identification of other standards (e.g., standards for quality assurance, conduct of operations, etc.) will be performed by specially constituted teams formed by the PMT in support of the PSAR."

A multi-discipline ISM team was specially constituted. The need to establish this team, the selection of an appropriate chairperson, and the scope of discipline involved were confirmed at the PMT meeting held October 25, 2001. The team lead selected knowledgeable individuals from each required discipline who were currently on the list of qualified individuals (LQI). The team lead also used subject matter experts (SMEs) as needed.

As the proposed changes do not involve engineering/design, manufacture/fabrication, and construction standards, the ISM team does not include specific work activity experts, hazard assessment experts, hazard control experts, or standards experts who would typically be assigned to an ISM team.

The table below lists the team members and subject matter experts.

Name	Title/Qualification	Department	Team Role
John Hinckley	Pretreatment Hazard & Safety Analysis Lead / LQI	ES&H/ Safety Analysis	Lead/Chair appointed by PMT
Dana Hyde	LAW Testing Lead / LQI	Commissioning and Training/Area Testing	Operations representation required by PMT
Steve Vail	Mechanical Systems Compliance Supervisor / LQI	Engineering/Mechanical Systems	Engineering representation required by PMT
Richard I. Smith	Principal Nuclear Engineer, LQI	BNI Nuclear Engineering/San Francisco	SME on safety and seismic categorization; former Chair
Thomas R. McDonnell	Safety & Regulatory Engineer, LQI	BNI Nuclear Engineering/San Francisco	SME on safety classification

3.3 Identify Work

The purpose of the identification of work step, as intended by the process described in 24590-WTP-GPP-SANA-002 (which implements SRD Appendix A and DOE/RL-96-0004) is so that hazards and hazardous situations inherent in the work can be identified and evaluated. The proposed change expands the scope of the WTP safety classification approach to ensure that it appropriately reflects the definition of Important to Safety in DOE/RL-96-0006. The proposed change does not directly affect the process, hazards, or control strategies. Hazards and hazardous situations are not applicable; therefore, control strategies with standards are not needed.

The result of this process step is that there was no “work” identified. The Hazard Evaluation, Development of Preferred Hazard Control Strategies, Design Basis Events (DBEs), Designation of Systems Structures, and Components (SSCs) Comprising the Hazard Control Strategy steps are not required. The process should continue with the Identification of Standards step.

3.4 Hazard Evaluation

Not required. See justification in section 3.2.

3.5 Development of Preferred Hazard Control Strategies

Not required. See justification in section 3.2.

3.6 Design Basis Events (DBEs)

Not required. See justification in section 3.2.

3.7 Designation of Systems Structures, and Components (SSCs) Comprising the Hazard Control Strategy

Not required. See justification in section 3.2.

3.8 Identification of Standards

The standards identification activity, as required by DOE/RL-96-0004, is used to identify a tailored set of standards and requirements that will assure adequate safety when implemented. The implementing standards selection criteria:

- Provides adequate safety
- Complies with applicable laws and regulations
- Conforms with top-level safety standards and principles

The demonstration of completion of this activity is provided in Attachment 6 of this ABCN.

3.9 Confirmation of Standards

Based on the results of the ISM process, the PMT recommended the selected revisions to the standards and safety criteria to the Project Safety Committee (PSC) Chair (Ref. PMT meeting on 8/15/02). The PSC Chair requested the PSC confirm the selected set of standards. The confirmation review approach is to distribute the ABCN for PSC review, present the approved ABCN at a PSC meeting, and reach consensus on approval of the ABCN. Comments by the PSC on the standards identification are required to receive formal disposition; however, no formal comments (PSC actions) on the standard were cited in the minutes (Ref PSC meeting on August 21, 2002).

3.10 Record Document Identification

Completion of this task is documented in PMT and PSC meeting minutes dated August 15, 2002, and August 21, 2002, respectively, and by PSC Chair signature on the ABCN.

3.11 Documentation

Following approval of the ABCN by the OSR, the results of the standards selection ISM process will be documented in the applicable sections of the SRD as indicated in the underline strikeout text in Attachments 1 and 2.

No other documentation other than described in section 3.9 is required.

4 Conclusions

In summary, the recommended approach provides numerous project benefits while maintaining a safe facility that meets all of the top-level DOE requirements.

5 References

Project Documents

4590-WTP-GPP-SANA-002, *Hazard Analysis, Development of Hazard Control Strategies, and Identification of Standards*

24590-WTP-ISMP-ESH-01-001, *Integrated Safety Management Plan*

24590-WTP-PSAR-ESH-01-001, *Preliminary Safety Analysis Report to Support Partial Construction Authorization*

24590-WTP-SRD-ESH-01-001-02, *Safety Requirements Document*

Codes and Standards

DOE/RL-96-0006. *Top-level Radiological, Nuclear, and Process Safety Standards and Principles for the RPP Waste Treatment Plant Contractor*, February 2001, US Department of Energy, Richland Operations Office, Richland, Washington.

Other Documents

RL/REG-98-17. *OSR Position on Tailoring for Safety*, Revision 2, 1 September 2001. US Department of Energy, Office of Safety Regulation, Richland, Washington.

RL/REG-2000-15. *OSR Position on the Achievement of Adequate Safety*, Rev 0, 28 September 2000. US Department of Energy, Office of Safety Regulation, Richland, Washington.

1. Introduction

The WTP project proposes to add the Risk Reduction Class (RRC) to the scope of Important to Safety (ITS) SSCs to afford a clearer demonstration of conformance with the definition of Important to Safety in DOE/RL-96-0006.

RRC SSCs typically correlate to the second level of defense in depth described in SRD Vol. II, Appendix B (which is derived from DOE G 420.1-1). As such, the RRC class of ITS SSCs minimizes challenges to the SDC and SDS SSCs, which prevent or mitigate the consequences of accidents. However, RRC items themselves are not credited in the accident analysis as controls to meet the radiological exposure standards or the requirements of SRD Appendix B Table 1.

2. Revised Safety Classification Definitions

The following definitions of SDC, SDS and RRC in SRD Safety Criterion 1.0-8 are proposed.

SDC Definition

Safety Design Class (SDC). SDC SSCs are the following:

1) SSCs whose safety function is to prevent workers or the maximally exposed member of the public from receiving a radiological exposure that exceeds the exposure standards defined in the SRD;
2) SSCs whose safety function is to prevent workers or the maximally exposed member of the public from receiving a chemical exposure that exceeds the exposure standards defined in the SRD;
3) SSCs that are credited for the prevention of a criticality event.

SDS Definition

Safety Design Significant (SDS). SDS SSCs are the following:

1) SSCs that are required to ensure that standards for normal operation are not exceeded;
2) SSCs whose failure would directly prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items); or
3) SSCs that are required to meet SRD Appendix B, *Implementing Standard for Defense in Depth*, Section 3.0, Table 1, Implementation of Defense in Depth by SSCs. (Such SDS SSCs are in addition to SSCs that are classified SDC to meet the Radiological Exposure Standards.)

RRC Definition

Risk Reduction Class (RRC). RRC SSCs are Important to Safety SSCs that are neither SDC nor SDS.

These definitions correspond to the following definition of Important to Safety from DOE/RL-96-0006.

> Structures, systems, and components that serve to provide reasonable assurance that the facility can be operated without undue risk to the health and safety of the workers and the public. It encompasses the broad class of facility features addressed (not necessarily

explicitly) in the top-level radiological, nuclear, and process safety standards and principles that contribute to the safe operation and protection of workers and the public during all phases and aspects of facility operations (i.e., normal operation as well as accident mitigation). This definition includes not only those structures, systems, and components that perform safety functions and traditionally have been classified as safety class, safety-related or safety-grade, but also those that place frequent demands on or adversely affect the performance of safety functions if they fail or malfunction, i.e., support systems, subsystems, or components. Thus, these latter structures, systems, and components would be subject to applicable top-level radiological, nuclear, and process safety standards and principles to a degree commensurate with their contribution to risk. In applying this definition, it is recognized that during the early stages of the design effort all significant systems interactions may not be identified and only the traditional interpretation of important to safety, i.e., safety-related may be practical. However, as the design matures and results from risk assessments identify vulnerabilities resulting from non-safety-related equipment, additional structures, systems, and components should be considered for inclusion within this definition.

3. Adequacy of WTP Safety Classification

The proposed three-tiered safety classification approach is adequate to ensure that the top-level standards, laws and regulations are met. Furthermore, BNI’s safety classification approach is comparable to or exceeds classification approaches used elsewhere in the DOE complex.

With the addition of Risk Reduction Class, top-level standards (i.e., DOE/RL-96-0004 and -0006) continue to be met. Table A-1 provides a detailed analysis of the application of the relevant top-level standards and principles to RRC SSCs. The RRC class broadens the scope of ITS SSCs for the WTP such that the definition of Important to Safety in DOE/RL-96-0006 is fully met.

The RRC class affords a broader spectrum of important-to-safety SSCs for the WTP than would be provided in a typical DOE nuclear facility applying the safety classifications of the Nuclear Safety Management rule 10 CFR 830 Subpart B and DOE-STD-3009-94. The existing WTP safety classification approach, comprising the SDC and SDS classes only, already exceeds the scope of safety SSCs defined in the rule and Technical Standard by including protection of workers against accident consequences. The new class RRC further broadens the scope of ITS for the WTP project by specifically identifying those SSCs that minimize challenges to SDC and SDS items. In addition, SSCs that are identified as significant contributors to safety by the analyses that confirm the facility accident risk goals are met are also classified as RRC. Therefore, the RRC classification responds to the broad definition of Important to Safety in DOE/RL-96-0006.

Furthermore, BNI’s proposed safety classification approach is comparable to, but exceeds, approaches taken elsewhere in the DOE complex. For example, at the Savannah River Site, SSCs that are neither safety class (SC) nor safety significant (SS) are referred to as Non-SC/SS Defense-in-Depth if additional controls are needed to demonstrate that the mitigated consequences to the public from accidents are significantly lower than the site evaluation guidelines. (BNI’s classification approach would afford similar protection to workers, as well.) Non-SC/SS Defense-in-Depth SSCs are classified as either Production Class or General Services Class; no standards are applied to these components beyond those used in commercial industrial applications.

4. Level of Radioactivity for ITS Boundaries

BNI's proposed definition of Risk Reduction Class includes those SSCs that protect against a release of significant amount of radioactivity, as illustrated in Table 1-3 of the proposed revision to the ISMP (Attachment 2 of this ABCN).

5. Codes and Standards for ITS SSCs

Because of the limited safety role that RRC SSCs perform, no design codes and standards beyond those used in commercial radiological and chemical industrial applications are required for RRC components. These design codes and standards will be reflected in the applicable procurement specifications, but would not be identified in the Safety Requirements Document (SRD). This position is consistent with the –0006 definition of ITS, which calls for grading of requirements commensurate with the contribution to risk of the SSCs. Section 7 of this attachment provides a further discussion of standards for RRC SSCs.

Typically, SDC/SDS SSCs have nuclear safety functions for event prevention or mitigation that need to be understood with clarity, which may differ in important respects from the functional requirements for similar equipment in non-nuclear applications; therefore, industry committees have developed specific guidance (standards) to assure the equipment/systems can meet these exceptional functions. Thus, identification, justification and approval of these standards are appropriate for SDC/SDS equipment.

Designating other SSCs as RRC provides added assurance that designers, constructors and operators are informed of their functional relevance to safety. However, the RRC class of equipment tends not to have exceptional functional requirements that require adoption of exceptional standards. Commercial design practices and standards used in the radiological and chemical industries provide technically appropriate guidance and are acceptable categorically.

6. Safety Assessment of RRC Classification

Safety Benefit of RRC Classification

Provision of the "Risk Reduction Class" designations in the SRD increases the number of plant items that are under the purview of the SRD, and thus enhances safety.

Although RRC SSCs are not specifically credited in the evaluation of the frequency and consequences of design basis events, they nevertheless will have an impact on the actual frequency and consequences. The PSARs identify the SSCs that have been classified as RRC in each WTP facility. Although other SDC/SDS SSCs are credited in the DBE analysis, these RRC SSCs will afford additional preventive or mitigative functions.

Barrier Integrity

The proposed definition of RRC ensures that all SSCs that comprise a physical barrier against a release of a significant amount of radioactive material will be classified as ITS. Those SSCs that comprise a physical barrier against a release of radioactive material and are credited for preventing workers or the public from receiving a radiological exposure that exceeds the exposure standards in the SRD will be classified as SDC. Those SSCs that comprise a physical barrier against a release of radioactivity and perform a significant Defense in Depth role, (i.e. –

are required to meet the requirements of SRD Appendix B, Table 1), are classified as SDS. Those SSCs that comprise additional physical barriers against a release of a significant amount of radioactive material, but which are not required to meet the radiological exposure standards and which do not perform a significant Defense in Depth role, will be classified as RRC.

Engineering specifies the codes and standards used in the design and procurement of RRC SSCs that ensure the integrity of the boundaries retaining radioactivity. These codes and standards do not need to be identified in the SRD and do not require DOE approval.

This approach is consistent with DOE-STD-3009-94 CN2,[1] which states:

> By virtue of application of the graded approach, the majority of the engineered features in a facility will **not** be identified in the categories of safety-class or safety-significant SSCs **even though they may perform some safety functions**. However, such controls noted as a barrier or preventive or mitigative feature in the hazard and accident analyses must not be ignored in managing operations. Such a gross discrepancy would violate the safety basis documented in the DSA even if the controls are not designated safety-class or safety- significant, because programmatic commitments extend to these SSCs as well. For example, the commitment to a maintenance program means that the preventive and mitigative equipment noted as such in the DSA hazard analysis are included in the facility maintenance program. As a minimum, all aspects of defense in depth identified must be covered within the relevant safety management programs (e.g., maintenance, quality assurance) committed to in the DSA. The **details** of that coverage, however, are **developed in the maintenance program as opposed to in the DSA**.[2] Facility operators are expected to have noted the relative significance of these engineered features and have provided for them in programs, in keeping with standard industrial practice, based on the importance of the equipment. It is the fact of coverage that is relevant to the facility safety basis. The details of this programmatic coverage (i.e., exact type of maintenance items and associated periodicities) are not developed in or part of the DSA.
> *[Emphasis added.]*

7. Adequacy of SRD Safety Criteria for SSCs Classified as RRC

Table A-1 demonstrates the adequacy of the implementation of SRD Safety Criteria related to top-level standards for RRC SSCs. The Safety Criteria (SC) whose Regulatory Basis invokes DOE/RL-96-0006 are listed in the table. The right-hand column evaluates the consistency of the proposed safety classification approach for WTP against the SCs and associated top-level requirements.

8. Reliability of RRC SSCs

For design and procurement, commercial quality and standard engineering requirements are adequate to ensure that RRC SSCs will perform their safety function. (This approach was validated during ISM Cycle 2.) However, to ensure that the reliability of installed RRC SSCs remains high throughout their operating lifetime, they will be "captured" as configured items. Attachment 2 of the revised ABCN adds three new attributes to the proposed list in ISMP section 1.3.10 that address maintenance and configuration control to be applied to RRC SSCs in service.

---

1 DOE-STD-3009-94, *Preparation Guide for U.S Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*. Change Notice No. 2, U.S. Department of Energy, Washington, DC, April 2002.

2 DSA = Documented Safety Analysis

Maintenance and inspection requirements for RRC SSCs will be determined during ISM Cycle 4 and documented in the Final Safety Analysis Report.

9. Level of Detail of RRC SSCs in PSAR

SRD Vol. II Safety Criterion 4.1-2 states, in part:

> "Structures, systems, and components designated as Important to Safety shall be designed, fabricated, erected, constructed, tested, inspected, and maintained to quality standards commensurate with the importance of the safety functions to be performed."

DOE/RL-96-0006 defines "safety function" as follows:

> "Any function that is necessary to ensure (1) the integrity of the boundaries retaining the radioactive materials, (2) the capability to place and maintain the facility in a safe state, or (3) the capability to prevent or mitigate the consequences of facility conditions that could result in radiological exposures to the general public or workers in excess of appropriate limits."

RRC SSCs are not credited to prevent or mitigate the consequences of accidents that could result in individuals exceeding exposure standards. However, RRC SSCs may be provided to address the first and second parts of the definition of "safety function," to the extent that they minimize challenges to SDC/SDS SSCs. The importance of the safety functions to be performed by RRC SSCs is much less than the importance of the safety functions of SDC and SDS SSCs.

At this stage, RRC SSCs have not been designed in great detail; however, the ongoing design process will develop such details. Given that RRC SSCs are not credited in the accident analysis and that they afford an additional layer of protection than typically provided by safety SSCs in other DOE facilities, detailed design information is not needed at the Construction Authorization Request stage. It is sufficient that the PSAR identifies the SSCs that are classified as RRC, their attributes and their safety functions as provided in the table in Chapter 3 of the PSAR.

DOE/RL-96-0003, Rev. 2, section 4.3.2, provides criteria on the content to be provided in the PSAR. The relevant criteria are as follows:

4. Description of planned facility operations.
5. Description of facility structures, systems, and components including those designated as important to safety.
7. Design data and design drawings to support descriptions in 5, above.
8. Analysis of radiological, nuclear, and process hazards for the design.
9. Description of facility features and functions provided to control the radiological, nuclear, and process hazards.
15. An analysis of the safety basis for the facility (safety envelope) in terms of physical design, structures with prescribed safety functions, systems with prescribed safety functions, equipment with prescribed safety functions, operating modes, operating conditions, off-normal internal events considered, external events considered, assumptions made, uncertainties in data and analyses, safety limits, and operating limits.

The design information provided in the PSAR is more than adequate to meet the content requirements of DOE/RL-96-0003. The level of detail provided is commensurate with the importance of the safety functions to be performed; therefore, the PSAR is responsive to Safety Criterion 4.1-2. Furthermore, the attributes of RRC SSCs are described in the proposed revision to ISMP section 1.3.10. Therefore, at this stage of the design, the PSAR provides adequate information regarding the RRC items.

It is also noted that footnote 4 of RL/REG-97-13, Rev. 8, *Contractor-Initiated Change(s) to the Authorization Basis*, states: "Safety Functions for Safety Design Class and Safety Design Significant SSCs typically are described in Chapter 4 of the Safety Analysis Report as are descriptions of how the SSC meets its respective safety function. Safety Functions of Risk Reduction Class (RRC) SSCs typically are described in Chapter 3 of the Safety Analysis Report." Thus, OSR guidance contemplates a lower level of design detail for RRC SSCs than for SDC and SDS SSCs and that RRC SSCs are not discussed in PSAR Chapter 4.

10. Standards for RRC SSCs

Because the relative importance of the safety functions of RRC SSCs is lower than that of items classified as SDC and SDS and the procurement process is rigorous, standards identification is not necessarily required to assure adequate product quality and reliability.

The first attribute for RRC SSCs listed in proposed ISMP section 1.3.10 (see ABCN –029) states: "In accordance with QAM compliance with DOE Order 414.1A, commercial grade quality requirements are applied to the SSC." Typically, RRC SSCs will be procured as follows. Based on the safety case requirements identified in the Standards Identification Process Database (SIPD) and other design criteria, Engineering will determine the requirements that a particular RRC SSC must meet (including any codes and/or standards selected and documented in the equipment specifications). Typically, vendor catalogs will be reviewed to identify commercially available hardware that meets the requirements, and the item will be ordered from the catalog. Upon receipt, Construction QC will verify that the procured item meets the purchase order requirements.

In some cases, vendors may apply recognized industry codes and standards in designing and fabricating the RRC components, even though WTP Engineering has not specified them. Competitive economic pressures require the manufacture of standard commercial hardware to be of very high quality. In fact, commercially acceptable hardware typically exhibits levels of reliability comparable to that of ITS equipment, provided that:

- the expected operational envelope for the SSC conforms to the range of process and environmental conditions anticipated by the vendor and normally employed in comparable processes by other customers, and
- a comprehensive, reliability-based approach is used to identify post-installation maintenance and testing requirements for these SSCs and the formal implementation of these requirements is controlled programmatically. The response to OSR Question ABCN-ESH-029-12 commits that WTP will have such a program for RRC SSCs.

11. Treatment of RRC SSCs in Evaluation of Proposed Facility Changes

Commencing with operations authorization (when the USQ process becomes effective), <u>any</u> proposed change to the facility described in the SAR will be evaluated as a potential USQ, regardless of the safety classification of the SSCs proposed to be modified.

The ABCN revises only the first test for a USQ in Safety Criterion 7.4-1 dealing with malfunction of equipment, as follows:

"A situation involves a USQ if:

1) the probability of occurrence or the radiological or chemical consequences of an accident or malfunction of equipment ~~Important to Safety~~ **designated as SDC or SDS**, previously evaluated in the facility safety analyses or other related safety analysis and evaluations not yet included in the updated facility analysis, may be increased."

SDC or SDS SSCs are specifically credited in the control strategies for postulated accidents, as documented in the safety analysis report. RRC SSCs are not credited in the safety analyses. Thus, an increase in the probability of malfunction of RRC SSCs should not be a USQ. Furthermore, the second and third tests for a USQ in Safety Criterion 7.4-1 are still applicable to RRC SSCs. As a practical matter, this change maintains the current commitment regarding USQ determinations. If malfunction of RRC equipment could result in an accident (e.g., failure of an vessel that contains radioactivity), such that an increase in the probability of malfunction results in an increase in the probability of an accident in the SAR, it would be a USQ. An RRC equipment malfunction of a different type than evaluated in the SAR would also be USQ, per the second test.

12. Environmental Qualification

As stated in the proposed change to the ISMP (Attachment 2 of ABCN –029), commercial quality requirements are applied to RRC SSCs, and RRC SSCs are normally designed to standard engineering requirements. Thus, design and procurement of RRC SSCs follow normal industrial practices. Standard industrial practice does not typically mandate qualification of electrical equipment for harsh post-accident environments. This is justified because RRC SSCs are classified as such to provide additional assurance that challenges to SDC and SDS SSCs specifically credited to prevent and mitigate accidents are minimized. Thus, once an accident occurs, RRC SSCs do not need to remain operable. Therefore, there is no benefit to qualifying RRC SSCs for a post-accident harsh environmental conditions in accordance with 10 CFR 50.49 and IEEE 323-83.

Nevertheless, RRC SSCs will be specified and procured for their anticipated service conditions. Commercial grade electrical equipment typically is designed to remain functional under "mild" environmental conditions found in industrial facilities. Thus, RRC electrical equipment can usually be purchased as commercial grade with assurance that it will withstand the service conditions. If an RRC electrical SSC is to be located in an environment that exceeds "mild" conditions, further information will be obtained from the vendor to ensure proper functionality of the equipment. Furthermore, as noted above, a predictive/preventive maintenance program for RRC SSCs will be developed that includes monitoring and trending of the condition of these SSCs throughout their operating life. Thus, potential degradation of RRC SSCs due to environmental conditions will be detected, evaluated and corrected, as necessary.

Table A-1
Evaluation of RRC against SRD Safety Criteria and Corresponding DOE/RL-96-0006 Requirements

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
3.3.1, Public Protection 3.3.2, Worker Protection	Measures in the design and operations of the facility to protect the public against accident conditions should be evaluated against acceptable guidelines to demonstrate that they perform their intended purpose with high confidence. Measures in the design and operations of the facility to protect the workers against accident conditions should be evaluated against acceptable guidelines to demonstrate that they perform their intended purpose with high confidence.	1.0-8	….Important to Safety includes SSCs designated as Safety Design Class, Safety Design Significant, and Risk Reduction Class. **Safety Design Class (SDC).** Safety Design Class SSCs are the following: 1) SSCs whose safety function is to prevent workers or the maximally exposed member of the public from receiving a radiological exposure that exceeds the exposure standards defined in the SRD; 2) SSCs whose safety function is to prevent workers or the maximally exposed member of the public from receiving a chemical exposure that exceeds the exposure standards defined in the SRD; or 3) SSCs that are credited for the prevention of a criticality event. **Safety Design Significant (SDS).** Safety Design Significant SSCs are the following: 1) SSCs that are required to ensure that standards for normal operation are not exceeded; 2) SSCs whose failure would directly prevent Safety Design Class SSCs from performing their safety function (e.g., Seismic II/I items); or 3) SSCs that are required to meet SRD	SDC and SDS SSCs protect workers and the public against the consequences of accidents.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			Appendix B, *Implementing Standard for Defense in Depth,* Section 3.0, Table 1, *Implementation of Defense in Depth by SSCs*. (such SDS SSCs are in addition to SSCs that are classified SDC to meet the Radiological Exposure Standards) **Risk Reduction Class (RRC).** RRC SSCs are Important to Safety SSCs that are neither SDC nor SDS.	

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
4.1.1.3, Control	Normal operation, including anticipated operational occurrences, maintenance, and testing, should be controlled so that facility and system variables remain within their operating ranges and the frequency of demands placed on structures, systems, and components important to safety is small.	4.3-4	Important to Safety instrumentation and controls shall be provided to monitor variables and systems and control systems and components over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate public and worker safety by compliance to the standards of Safety Criteria 2.0-1 and 2.0-2, including those variables and systems that can affect the performance of Important to Safety facility conditions. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. The instrumentation and controls provided shall provide the ability to detect off normal conditions, mitigate accidents, and place the facility in a safe state.	The implementing standard for SDC and SDS instrumentation and controls remains DOE O 420.1, §4.1.1.2. SRD Appendix A will be used to determine requirements for RRC instrumentation and controls. SRD Appendix A is the WTP project's implementation of the standards identification process required by DOE/RL-96-0004. RRC instrumentation and controls will ensure that facility and system variables remain within their operating ranges and the frequency of demands placed on SDC and SDS SSCs is small. Thus, the RRC class is responsive to this SC and the corresponding top-level requirement. The implementing standard for this safety criterion is the Control sub-principle of SRD Appendix B, *Implementing Standard for Defense in Depth*, which applies to all ITS SSCs, including RRC.
		7.0-2	Normal operation, including anticipated operational occurrences, maintenance, and testing, shall be controlled so that facility and system variables remain within their normal operating ranges and the frequency of demands placed on Important to Safety structures, systems, and components are small.	

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	Top-Level Requirement	SC	Safety Criterion	
4.1.1.5, Defense in Depth – Automatic Systems	Automatic systems should be provided that would place and maintain the facility in a safe state and limit the potential spread of radioactive materials when operating conditions exceed predetermined safety setpoints.	4.3-1	Engineered safety systems shall be designed (1) to initiate automatically the operation of appropriate systems to assure that specified acceptable design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of Important to Safety systems and components. The ability to manually initiate engineered safety systems shall be provided.	The implementing standard for this safety criterion is the Automatic Systems sub-principle of SRD Appendix B, *Implementing Standard for Defense in Depth*, which applies to all ITS SSCs, including RRC. RRC SSCs may provide automatic system response or may be SSCs such as monitors or alarms that alert operators to the necessity of taking manual action. Thus, the RRC class is responsive to this SC and the corresponding top-level requirement.
4.1.6.3, Operational Quality Assurance Programs	Operational quality assurance and control programs should be established by the Contractor to assist in ensuring satisfactory performance in facility activities important to safety.	7.3-5	Work shall be performed to established technical standards and administrative controls using approved instructions, procedures, or other appropriate means. Items shall be identified and controlled to ensure their proper use. Items shall be maintained to prevent their damage, loss, or deterioration. Equipment used for process monitoring or data collection shall be calibrated and maintained.	The SC and the corresponding top-level requirement are applicable to RRC. Quality Assurance requirements will be graded commensurate with the hazard.
4.2.2.2, Common-Mode/ Common-Cause Failure	Design provisions should be included to limit the loss of safety functions due to damage to several structures, systems, or components important to safety resulting from a common-cause or common-mode failure.	4.1-3	This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) that are Important to Safety and have NPH safety functions. SSCs designated as Important to Safety (i.e., Safety Design Class and Safety Design Significant) shall be designed to withstand the effects of NPH events such as earthquakes, wind, and floods without loss of capability to perform specified safety functions required as the result of the NPH events. This includes both the front line and	By definition, RRC SSCs do not have NPH safety functions; therefore, this SC does not apply to RRC.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			support systems that must function for a NPH event such that the public, collocated worker, or facility worker exposure standards of Safety Criterion 2.0-1 or 2.0-2 are not exceeded. SSCs that are designated Safety Design Class (excepting those so designated based solely on chemical hazards) and that are required to perform a safety function as a result of a given NPH shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. These SSCs are designated Seismic Category I (SC-I) for earthquakes and Performance Category 3 (PC-3) for other NPH. SSCs that are designated Safety Design Significant (excepting those so designated based solely on chemical hazards) whose continued function is not required for an NPH event, but whose failure as a result of an NPH event could reduce the functioning of a Safety Design Class SSC such that exposure standards might be exceeded, shall be designed to withstand the NPH loadings of that NPH as provided in Table 4-1. For these SSCs, however, for seismic response only, credit may be taken for inelastic energy absorption per Table 2-4 of DOE-STD-1020-94. These SSCs are designated SC-II for earthquakes and PC-3 for other NPH. For any SSC included under this criterion, other NPH loads (for which the SSC has no safety function) may be taken from Safety Criterion 4.1-4 and Table 4-2 in lieu of Safety Criterion 4.1-3 and Table 4-1.	

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
		4.1-4	This criterion addresses natural phenomena hazards (NPH) design for structures, systems, and components (SSCs) without NPH safety functions. This criterion also addresses NPH design for SSCs with an NPH safety function associated solely with protection of workers and members of the public from exposure to chemical hazards. SSCs that may be important to the safety of the RPP WTP shall be designed to withstand the effects of NPH such as earthquakes, wind, and floods. The SSCs included under this criterion are: 1. Safety Design Class (SDC) and Safety Design Significant (SDS) SSCs that do not have an NPH safety function, 2. SSCs that have a seismic safety function solely because they protect workers and members of the public from exposure to chemical hazards, 3. Risk Reduction Class (RRC) SSCs that provide primary confinement of significant inventories of radioactive materials but in amounts less than quantities that require an SDC or SDS designation, and 4. RRC SSCs that do not provide primary confinement of significant inventories of radioactive materials. SSCs included under items 1, 2, or 3 (above) are designated Seismic Category III (SC-III) for earthquakes and Performance Category 2 (PC-2) for other NPH, and shall be designed to withstand the NPH loadings	The revised SC assigns RRC SSCs to Seismic Categories and Performance Categories appropriate to their potential seismic failure consequences.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			as provided in Table 4-2. SSCs designated as RRC that do not provide primary confinement of significant inventories of radioactive materials under item 4 above shall be designated Seismic Category IV (SC-IV) for earthquakes and Performance Category 1 (PC-1) for other NPH, in accordance with the PC-1 requirements of DOE-STD-1020-94.	
		4.3-3	Important to Safety engineered safety systems shall be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed. Design provisions should be included to limit the loss of safety functions due to damage to several structures, systems, or components Important to Safety resulting from a common-cause or common-mode failure. The protection system shall be designed to permit periodic testing of its functioning when the facility is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.	SRD Appendix A will be used to determine reliability and inservice testability requirements for RRC SSCs commensurate with their safety functions, as well as for SDC and SDS SSCs. To ensure that the reliability of installed RRC SSCs remains high throughout their operating lifetime, they will be "captured" as configured items. This ABCN adds three new attributes to the proposed list in ISMP section 1.3.10 that address maintenance and configuration control to be applied to RRC SSCs in service. Thus, the RRC class is responsive to this SC and the corresponding top-level requirement. The WTP Integrated Safety Management (ISM) program evaluates potential common-mode/common-cause failures without regard to the safety classification of SSCs. The ISM program investigates potential functional, spatial and institutional dependencies. Identification of common cause failures considers the following potential events. ▪ Loss of electrical power ▪ Failure of multiple systems due to process upsets ▪ Failure of common support systems or shared components

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
				▪ External (natural phenomena) hazards ▪ Internal hazards – fires, flooding, missiles, and overpressure events.
4.2.2.3, Safety System Design and Qualification	Structures, systems, and components important to safety should be designed and qualified to function as intended in the environments associated with the events for which they are intended to respond. The effects of aging on normal and abnormal functioning should be considered in design and qualification.	4.1-2	Structures, systems, and components designated as Important to Safety shall be designed, fabricated, erected, constructed, tested, inspected, and maintained to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. Appropriate records of the design, fabrication, erection, and testing of structures, systems, and components designated as Important to Safety shall be maintained through deactivation of the facility. Items and processes shall be designed using sound engineering/scientific principles and appropriate standards. Design features that enhance the margin of safety through simplified, inherently safe, passive, or other highly reliable means to accomplish the specified safety function should be employed to the maximum extent practical. Design work, including changes, shall incorporate applicable requirements and design bases. Design interfaces shall be identified and controlled. The adequacy of	The safety criterion encompasses all Important to Safety SSCs, including RRC items. It was determined during ISM Cycle 2 that no special design or procurement requirements were needed for RRC SSCs to meet the exposure standards. Therefore, if generally recognized codes and standards are desired to be applied to RRC SSCs, the codes and standards are invoked in procurement specifications and not in the SIPD.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			design products shall be verified or validated by individuals or groups other than those who performed the work. Verification and validation work shall be completed before approval and implementation of the design.	
		4.4-2	Structures, systems, and components Important to Safety shall be designed and qualified to function as intended in the environments associated with the events for which they are intended to respond. The effects of aging on normal and abnormal functioning shall be considered in design and qualification.	The implementing standard for SDC and SDS SSCs remain 10 CFR 50.49 and IEEE 323-83. SRD Appendix A will be used to determine the particular environmental qualification requirements for RRC SSCs, as well as for SDC and SDS SSCs. Design and procurement of RRC SSCs follow normal industrial practices. Standard industrial practice does not typically mandate qualification of electrical equipment for harsh post-accident environments. This is justified because RRC SSCs are classified as such to provide additional assurance that challenges to SDC and SDS SSCs specifically credited to prevent and mitigate accidents are minimized. Thus, once an accident occurs, RRC SSCs do not need to remain operable. Therefore, there is no benefit to qualifying RRC SSCs for a post-accident harsh environmental conditions in accordance with 10 CFR 50.49 and IEEE 323-83. Nevertheless, RRC SSCs will be specified and procured for their anticipated service conditions. Commercial grade electrical equipment typically is designed to remain functional under "mild" environmental conditions found in industrial facilities. Thus, RRC electrical equipment can usually be purchased as commercial grade with assurance that it will withstand the service conditions. If an RRC electrical SSC is to be located in an environment that exceeds "mild" conditions,

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
				further information will be obtained from the vendor to ensure proper functionality of the equipment. Furthermore, as noted above, a predictive/preventive maintenance program for RRC SSCs will be developed that includes monitoring and trending of the condition of these SSCs throughout their operating life.
4.2.6.3, Safety Status	Parameters to be monitored in the control room should be selected and their displays should be arranged to ensure that operators have clear and unambiguous indications of the status of facility conditions important to safety, especially for the purpose of identifying and diagnosing the actuation and operation of a system or components important to safety.	4.3-6	The possibility of human error in facility operations shall be taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions and by providing means for detecting and correcting or compensating for error. The parameters to be monitored in control areas shall be selected and their displays arranged to ensure operators have clear and unambiguous indication of the status of the facility. The parameters and displays shall facilitate monitoring and the initiation and operation of systems designated as Important to Safety.	The safety criterion encompasses all Important to Safety SSCs, including RRC items.
4.2.7.1, Reliability	Reliability targets should be assigned to structures, systems, and components or functions important to safety. The targets should be consistent with the roles of the structures, systems, and components or functions in different accident conditions. Provision should be made for appropriate testing and inspection of structures, systems, and components for which reliability targets have been set.	4.4-4	Structures, systems, and components Important to Safety shall be designated, designed and constructed to permit appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin. Systems and components designated as Important to Safety that are located in closed cells where access is not possible during facility operation or scheduled shutdown periods shall be designed and constructed to standards aimed at ensuring their suitability for the entire service life with an adequate safety margin.	SRD Appendices A and E will be used to determine the particular inspection, testing and maintenance requirements for RRC SSCs, as well as for SDC and SDS SSCs. Requirements typically imposed on ITS SSCs are of a higher level than those used for non-ITS SSCs to ensure that they will function as designed, given their ITS classification and role. RRC SSCs are not credited for preventing and mitigating accidents; however, they do have a safety function in minimizing challenges to SDC and SDS SSCs. To ensure that the reliability of installed RRC SSCs remains high throughout their operating lifetime, they will be "captured" as configured items, and their maintenance and inspection program will be

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			Alternately, provisions may be made for remote replacement, standby cells, or equipment or other methods capable of ensuring a serviceable facility with adequate safety for the duration of the intended operating life.	enhanced beyond those employed for non-ITS items. This ABCN revision adds three new attributes to the proposed list in ISMP section 1.3.10 that address maintenance and configuration control to be applied to RRC SSCs in service.
		7.6-3	The maintenance program for Important to Safety Structures, systems and components shall clearly define: (1) The Important to Safety structures, systems, and components that comprise the facility (2) The requirements of the maintenance program that are derived from the program elements listed in Safety Criterion 7.6-4 (3) The management systems used for those activities, including the means for monitoring and measuring the effectiveness of the program and the management of maintenance backlog (4) The assignment of responsibilities and authority for all levels of the maintenance organization (5) Mechanisms to feedback such relevant information as trend analysis and instrumentation performance/reliability data in order to identify necessary program modifications (6) Provisions for identifying and evaluating possible component, system design, occupational safety and health, or other relevant problems and implementation of a self-assessment program	As noted above, RRC SSCs will be captured in the maintenance program. As committed in the revised ABCN, • Appropriate preventive and predictive maintenance will generally be applied to RRC equipment. • Monitoring of performance and condition and trending of the need for maintenance will also generally be applied to RRC SSCs. This monitoring and trending will provide input to the schedule and scope of the preventive and predictive maintenance and will also identify the need for replacement or modification of RRC SSCs

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			(7) Performance indicators and criteria to be utilized to measure equipment, systems, and personnel effectiveness in maintenance activities (8) Interfaces between maintenance and other organizations (e.g., involving operations, engineering, quality, and safety) (9) Quantitative reliability target values for systems and components to start or run, when such values are credited in safety analysis (10) Appropriate authorization is received before modification starts on a safety instrumented system (11) Assessment of impact of the modification on the functionality of the safety instrumented system is performed, to ensure functionality is not impaired	
4.2.7.2, Availability, Maintainability and Inspectability	Structures, systems and components important to safety should be designated, designed and constructed for appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin.	4.4-4	Structures, systems, and components Important to Safety shall be designated, designed and constructed to permit appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin. Systems and components designated as Important to Safety that are located in closed cells where access is not possible during facility operation or scheduled shutdown periods shall be designed and constructed to standards aimed at ensuring their suitability for the entire service life with an adequate safety margin.	See evaluation for top-level requirement 4.2.7.1, above.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			Alternately, provisions may be made for remote replacement, standby cells, or equipment or other methods capable of ensuring a serviceable facility with adequate safety for the duration of the intended operating life.	
4.2.8.1, Testing Program	A pre-operational testing program should be established and followed to demonstrate that the entire facility, especially items important to safety, have been constructed and function according to the design intent, and to ensure that weaknesses are detected and corrected.	6.0-1	A pre-operational testing program shall be established and followed to demonstrate that Important to Safety structures, systems and components have been properly constructed and can perform their specified functions. The program shall provide for the detection, tracking, and correction of deficiencies.	The safety criterion encompasses all Important to Safety SSCs, including RRC items.
4.2.8.3, Safety Systems Data	During pre-operational testing, detailed diagnostic data should be collected on systems and components important to safety and the initial operating parameters of the systems and components should be recorded.	6.0-3	During pre-operational testing, detailed diagnostic data shall be collected on systems and components designated as Important to Safety and the initial operating parameters of the systems and components shall be recorded.	The safety criterion encompasses all Important to Safety SSCs, including RRC items.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
4.2.8.4, Design Operating Characteristics	During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components important to safety should be determined and documented. Operating points should be adjusted to conform to values in the design basis. Training procedures and limiting conditions for operation should be modified to accurately reflect the operating characteristics of the systems and components as built.	6.0-4	During the pre-operational testing program, the as-built operating characteristics of process systems, and systems and components designated as Important to Safety shall be determined and documented. Operating points shall be adjusted to conform to values in the design basis. Training procedures and Limiting Conditions for Operation (when provided) shall be modified, if necessary, to accurately reflect the operating characteristics of the systems and components as built.	LCOs will not apply to RRC SSCs. All RRC items will be checked and their performance verified per RAMI program (see evaluation against top-level requirement 4.2.7.1, SC 7.6-3). Testing of RRC SSCs will be controlled in a similar fashion as for non-ITS SSCs. The configuration of RRC SSCs will be managed as part of the technical baseline, including replacement parts evaluation, setpoint control, and design change control. Monitoring of performance and condition and trending of the need for maintenance will also generally be applied to RRC SSCs. This monitoring and trending will provide input to the schedule and scope of the preventive and predictive maintenance and will also identify the need for replacement or modification of RRC SSCs.
4.3.1.7, Access to Technical Safety Support	Throughout the life of the facility, the Contractor should have access to engineering and technical support personnel, who are competent in all disciplines important to safety.	7.2-1	Programs providing for continual training and qualification for operations, maintenance, and technical support personnel, to enable them to perform their duties safely and efficiently, shall be developed and implemented utilizing a tailored approach.	No change is necessary for this safety criterion to implement the requirements for RRC.
4.3.5.1, Operational Testing, Inspection, and Maintenance	Structures, systems, and components important to safety should be the subject of appropriate, regular preventive maintenance, inspection, and testing and servicing when needed, to ensure that they remain capable of meeting their design requirements throughout the life of the facility. Such activities should be carried out in accordance with written procedures supported by quality assurance measures.	7.6-2 7.6-3	The maintenance program shall contain provisions sufficient to preserve, predict, and restore the availability, operability, and reliability of structures, systems, and components designated as Important to Safety. [Same as above]	The safety criterion encompasses all Important to Safety SSCs, including RRC items. The safety criterion encompasses all Important to Safety SSCs, including RRC items.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
4.3.6.1, Security	Adequate provisions for facility security and physical protection of structures, systems, and components important to safety should be provided.	4.1-6	Adequate provisions for facility security and physical protection of structures, systems, and components Important to Safety shall be provided.	The safety criterion encompasses all classes of Important to Safety SSCs, including RRC.
6.0, Glossary	**defense in depth:** The fundamental principle underlying the safety technology of the facility centered on several levels of protection including successive barriers preventing the release of radioactive materials to the workplace or environment. Human aspects of defense in depth are considered to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, operating limits, personnel qualification and training, and safety program. Design provisions, including both those for normal facility systems and those for systems important to safety help to: 1) prevent undue challenges to the integrity of the physical barriers; 2) prevent failure of a barrier if it is challenged; 3) where it exists, prevent consequential damage to multiple barriers in series; and 4) mitigate the consequences of accidents. Defense in depth helps to assure that two basic safety functions (controlling the process flow and confining the radioactive material) are preserved and that radioactive materials do not reach the worker, public, or the environment.	4.1-1	The facility design shall provide for the prevention and mitigation of the risks associated with radiological and chemical material inventories and energy sources. The facility design shall include consideration of normal operation (including startup, testing and maintenance), anticipated operational occurrences, external events, and accident conditions. Prevention shall be the preferred means of achieving safety. Defense-in-depth shall be applied commensurate with the hazard to provide multiple physical and administrative barriers against undue radiation and chemical exposure to the public and workers.	This safety criterion applies to RRC SSCs.
		4.2-1	The facility shall be designed to retain the radioactive and hazardous material through a conservatively designed confinement system for normal operations, anticipated operational occurrences, and accident conditions. The confinement system shall protect the worker and public from undue risk of releases such that the radiological and chemical exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.	This safety criterion applies to RRC SSCs.
		4.3-1	Engineered safety systems shall be designed (1) to initiate automatically the operation of	The implementing standards for SDC and SDS SSCs for this safety criterion are unchanged. For

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			appropriate systems to assure that specified acceptable design limits are not exceeded as a result of anticipated operational occurrences and (2) to sense accident conditions and to initiate the operation of Important to Safety systems and components. The ability to manually initiate engineered safety systems shall be provided.	RRC SSCs, the implementing standards are SRD Appendix A and the Automatic Systems sub-principle of SRD Appendix B, *Implementing Standard for Defense in Depth*. See the evaluation for top-level requirement 4.1.1.5.
		4.3-2	When single failure protection is required, Important to Safety engineered safety systems shall be designed to assure that the effects of natural phenomena (including lightning), and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.	This safety criterion is unchanged by ABCN –029; however, sections 6.4 and 6.5 of the SRD, which tailor implementing standards ANSI/ANS-58.9-1981 and IEEE STD 379-1994, single failure criteria are related only to SDC and SDS SSCs. This is consistent with Table 1 of SRD Appendix A, which requires application of the single failure criteria for SL-1 events and consideration of the single failure criteria for SL-2 events.
		4.3-4	Important to Safety instrumentation and controls shall be provided to monitor variables and systems and control systems and components over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate public and worker safety by compliance to the standards of Safety Criteria 2.0-1 and 2.0-2, including those variables and systems	The implementing standards for SDC and SDS instrumentation and controls are unchanged. SRD Appendix A will be used to determine requirements for instrumentation and controls classified as RRC, as well as those classified SDC and SDS. See evaluation for top-level requirement 4.1.1.3.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			that can affect the performance of Important to Safety facility conditions. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. The instrumentation and controls provided shall provide the ability to detect off normal conditions, mitigate accidents, and place the facility in a safe state.	
		4.3-5	When single failure protection is required, Important to Safety protection systems shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.	See evaluation for SC 4.3-2.
		4.3-6	The possibility of human error in facility operations shall be taken into account in the design by facilitating correct decisions by operators and inhibiting wrong decisions and by providing means for detecting and correcting or compensating for error. The parameters to be monitored in control areas shall be selected and their displays arranged to ensure operators have clear and unambiguous indication of the status of the	This safety criterion is applicable to RRC parameters and displays.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			facility. The parameters and displays shall facilitate monitoring and the initiation and operation of systems designated as Important to Safety.	
6.0, Glossary	**reliability targets**: Quantified probabilistic expectations that a component, equipment, or system will perform its intended function satisfactorily under given circumstances, such as environmental conditions, limitations as to operation time, and frequency and thoroughness of maintenance for a specified period of time. Identified important to safety items are expected to perform their function satisfactorily through all design basis accident conditions.	4.2-3	Codes and standards for Important to Safety vessels and piping should be supplemented by additional measures (such as erosion/corrosion programs and piping in-service inspections) to mitigate conditions arising that could lead to a release of radiological or chemical material that would exceed the worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2.	The safety criterion encompasses all Important to Safety vessels and piping, including RRC items.
		4.4-4	Structures, systems, and components Important to Safety shall be designated, designed and constructed to permit appropriate inspection, testing, and maintenance throughout their operating lives to verify their continued acceptability for service with an adequate safety margin. Systems and components designated as Important to Safety that are located in closed cells where access is not possible during facility operation or scheduled shutdown periods shall be designed and constructed to standards aimed at ensuring their suitability for the entire service life with an adequate safety margin. Alternately, provisions may be made for remote replacement, standby cells, or equipment or other methods capable of ensuring a serviceable facility with adequate safety for the duration of the intended	The implementing standards for SDC and SDS SSCs for this safety criterion are unchanged. For RRC SSCs, the implementing standards are SRD Appendices A and E. See the evaluations for top-level requirements 4.2.7.1 and 4.2.7.2.

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
			operating life.	
6.0, Glossary	**safety function**: Any function that is necessary to ensure (1) the integrity of the boundaries retaining the radioactive materials, (2) the capability to place and maintain the facility in a safe state, or (3) the capability to prevent or mitigate the consequences of facility conditions that could result in radiological exposures to the general public or workers in excess of appropriate limits.	N/A	None.	Engineering specifies the codes and standards used in the design and procurement of RRC SSCs that ensure the integrity of the boundaries retaining radioactivity. These codes and standards do not need to be identified in the SRD and do not require DOE approval. This approach is consistent with DOE-STD-3009-94 CN2, which states: "By virtue of application of the graded approach, the majority of the engineered features in a facility will **not** be identified in the categories of safety-class or safety-significant SSCs **even though they may perform some safety functions**. However, such controls noted as a **barrier** or preventive or mitigative feature in the hazard and accident analyses must not be ignored in **managing operations**. Such a gross discrepancy would violate the safety basis documented in the DSA even if the controls are not designated safety-class or safety-significant, because programmatic commitments extend to these SSCs as well. For example, the commitment to a maintenance program means that the preventive and mitigative equipment noted as such in the DSA[3] hazard analysis are included in the facility maintenance program. As a minimum, all aspects of defense in depth identified must be covered within the relevant safety management programs (e.g., maintenance, quality assurance) committed to in the DSA. The **details** of that coverage, however, are **developed in the maintenance program as opposed to in the DSA**.

[3] DSA = Documented Safety Analysis

DOE/RL-96-0006		Safety Requirements Document		Consistency of Revised WTP Safety Classification with Top-Level Standards
Section/Title	**Top-Level Requirement**	**SC**	**Safety Criterion**	
				Facility operators are expected to have noted the relative significance of these engineered features and have provided for them in programs, in keeping with standard industrial practice, based on the importance of the equipment. It is the fact of coverage that is relevant to the facility safety basis. The details of this programmatic coverage (i.e., exact type of maintenance items and associated periodicities) are not developed in or part of the DSA." [Emphasis added.]
None	N/A	4.2-2	Important to safety liquid and gaseous systems and components, including pressure vessels, tanks, heat exchangers, piping, and valves, shall be designed to retain their hazardous inventory such that the radiological and chemical worker or public exposure standards of Safety Criteria 2.0-1 and/or 2.0-2 are not exceeded.	This safety criterion is unchanged by ABCN –029.
None	N/A	4.2-4	Liquid and gaseous storage systems designated as Important to Safety shall have continuous monitoring to detect the loss or degradation of their safe storage function. As appropriate the following shall be monitored: temperature; pressure; radioactivity in ventilation exhaust and liquid effluent streams liquid levels tank chemistry; condensate and cooling water generation of flammable and explosive mixtures of gases	This safety criterion is unchanged by ABCN –029.